One Identity Manager 9.1.2

Web Designer Web Portal User Guide

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

One Identity Manager Web Designer Web Portal User Guide
Updated - 20 November 2023, 08:54

For the most recent documents and product information, see Online product documentation.

Contents

1

General tips and getting started

You can use the Web Portal to request and cancel products, and to renew current requests with limited lifetimes. If you own the respective entitlements, you can also approve requests and cancellations, perform attestation, view rule violations, and approve or deny exception approvals. You can also call up a wide range of statistics.

> NOTE: This guide describes the Web Portal with its factory settings. Your version of the Web Portal may be different because your Web Portal may have been customized.
>
> In addition, which Web Portal functionality is available to you is controlled by a role model in the database. This guide describes all the Web Portal functions. If you cannot find one of the functions described here in your Web Portal, it may be due to insufficient permissions. In this case, ask your administrator.

Tips for using the Web Portal

- Enable JavaScript in your browser for the Web Portal to work.
- You can configure and extend the Web Portal using the Web Designer.
- For optimal displaying of the graphical user interface, use a device with a minimum screen resolution of 1280 x 1024 pixels and at least 16-bit color depth. For mobile viewing, for example when using a tablet, use a device with a display size of at least 9.7 inches.
- Supported browsers:
    - Internet Explorer 11
    - Firefox (release channel)
    - Chrome (release channel)
    - Safari (current version)
    - Microsoft Edge (release channel)

Detailed information about this topic

- Logging in and out on page 28
- Navigation and use on page 32
- Displaying the address book on page 51

- Managing password questions on page 52
- Changing passwords on page 55
- Unlocking user accounts on page 56
- Editing your profile information on page 57
- Switching languages on page 58
- Enabling/disabling email notifications on page 58
- Personal dashboard settings on page 59
- Report subscriptions management on page 59
- Reports on page 62
- The user interface layout on page 69

Logging in and out

You must be logged onto the system to be able to work with the Web Portal. In order to login, you must know the URL of the Web Portal in your organization. Ask your system administrator for this information.

TIP: If you do not yet have an account, contact your manager.

NOTE: If you have forgotten your password and your account cannot be unlocked with the question-answer function, you can ask your manager for a passcode.

Detailed information about this topic

- First login/new account on page 28
- Logging in on page 29
- Logging in with security keys on page 30
- Logging in to the Password Reset Portal on page 30
- Logging off on page 32

First login/new account

If you do not already have a user account, you will have to create a new one.

To log onto the system for the first time

1. In the address line of your web browser, enter the Web address (URL) of the Web Portal to open the login page for the Web Portal.

TIP: By default, the URL is `http://<server name>/<application name>/`, where `<server name>` is the name of the server on which the Web Portal is installed.

2. Click **Create new user account** on the login page.
3. On the **Register a new user** view, complete at least the **Last name** and **First name** mandatory fields and enter your email address.
4. In the field next to **Security code**, enter the code displayed.

   TIP: If you cannot clearly identify the code displayed, click **Generate a different code** to display a new code.
5. Click **Save**.

   When the responsible manager has approved your account, you will receive an e-mail containing a link.
6. Open the confirmation email and click the link.
7. On the confirmation page, click **Confirm email address**.
8. Define your password and your password questions (see also, Changing passwords on page 55 and Managing password questions on page 52).
9. You can then log in using this information.

Related topics

- Logging in on page 29
- Changing passwords on page 55
- Managing password questions on page 52

Logging in

Open the Web Portal in a web browser.

If your system is also configured for two-factor authentication, other steps might be required to log in. For more information about logging in with your security key, see Logging in with security keys on page 30.

To log in to the Web Portal

1. In the address line of your web browser, enter the web address (URL) of the Web Portal.

   TIP: By default, the URL is http://<server name>/<application name>/, where `<server name>` is the name of the server on which the Web Portal is installed.
2. On the Web Portal login page, in the **Login name** field, enter your full user name.
3. In the **Password** field, enter your personal password.
4. Click **Log in**.

TIP: If you have forgotten your password, click **Forgot your password? Click here.**.

Then you are forwarded to the Password Reset Portal. For more information on this topic, see Changing passwords on page 55.

Related topics

- First login/new account on page 28
- Logging in with security keys on page 30
- Changing passwords on page 55
- Managing password questions on page 52

Logging in with security keys

If your system is appropriately configured and you own and have set up a security key, you can use it to log in to the Web Portal.

To log in to the Web Portal with a security key

1. In the address line of your web browser, enter the web address (URL) of the Web Portal.

   TIP: By default, the URL is http://<server name>/<application name>/, where `<server name>` is the name of the server on which the Web Portal is installed.

2. On the Web Portal's log in page, enter your login data.
3. Click **Log in**.
4. Follow the instructions (for example, plug your security key into your USB socket and then touch it).

   You will be automatically logged in.

Related topics

- First login/new account on page 28
- Logging in on page 29
- Security keys (WebAuthn) on page 75

Logging in to the Password Reset Portal

The Password Reset Portal helps you to change your main password, change several passwords of different user accounts, manage your password questions, and manage your security keys.

You can log in to the Password Reset Portal in three different ways:

- Use a passcode that you have received from your manager.
- Answer your personal password questions.
- Use your user name and personal password to log in to the Web Portal.

To log in to Password Reset Portal using an passcode

1. On the Web Portal's login page, click **Manage your passwords** or **Forgot your password?**. This opens the Password Reset Portal.

   The Password Reset Portal opens.

2. On the **Select how you want to authenticate yourself** page, select the option **I have a passcode** next to **Authentication method**.
3. In the **User name** field, enter your user name.
4. Click **Next**.
5. On the **Enter your passcode** page, in the **Passcode** field, enter your passcode.
6. In the field below **Enter the security code**, enter the CAPTCHA code displayed.

   TIP: If you cannot clearly identify the CAPTCHA code displayed, click **Generate a different code**. A new CAPTCHA code is then generated.

7. Click **Next**.

To log in to Password Reset Portal using your password questions

1. On the Web Portal's login page, click **Manage your passwords** or **Forgot your password?**.

   The Password Reset Portal opens.

2. On the **Select how you want to authenticate yourself** page, select the option **I want to answer my secret password questions** next to **Authentication method**.
3. In the **User name** field, enter your user name.
4. Click **Next**.
5. On the **Answer your password questions** page, enter the relevant answers to your password questions in the fields.
6. In the field below **Enter the security code**, enter the CAPTCHA code displayed.

   TIP: If you cannot clearly identify the CAPTCHA code displayed, click **Generate a different code**. A new CAPTCHA code is then generated.

7. Click **Next**.

To log in to Password Reset Portal using your current password

1. On the Web Portal's login page, click **Manage your passwords** or **Forgot your password?**.

   The Password Reset Portal opens.

2. On the **Select how you want to authenticate yourself** page, select the option **I log in with my current password** next to **Authentication method**.
3. In the **User name** field, enter your user name.
4. Click **Next**.
5. On the **I log in with my current password** page, enter your login information in the fields.
6. In the field below **Enter the security code**, enter the CAPTCHA code displayed.

   TIP: If you cannot clearly identify the CAPTCHA code displayed, click **Generate a different code.** A new CAPTCHA code is then generated.
7. Click **Next**.

Related topics

- First login/new account on page 28
- Logging in on page 29
- Logging off on page 32

Logging off

When you want to finish working with the Web Portal, log off from the system.

To log off from Web Portal

1. In the header, click (**Profile**) > **Log Off**.
2. In the **Log Off** dialog, confirm the prompt with **OK**.

   Your logoff was successful.

   TIP: Your system may be configured to log you off automatically if you are inactive for a long period of time.

Navigation and use

This chapter describes how you navigate through the Web Portal and how to utilize the Web Portal.

Detailed information about this topic

- Simple navigation on page 33
- Search on page 34
- Sorting on page 36

Simple navigation

Simple commands

Table 1: Overview of simple commands

Tab	Navigate between single elements
Enter or, if required, Space	Confirm input
Backspace	Navigate to previous page
Alt + Left arrow or Alt + Right arrow	Navigate to previous or next page

NOTE: Take into account that not all browsers behave the same.

Go to the home page

Table 2: Overview of key combinations for navigating

Tab	Navigate forward
Shift + Tab	Navigate backwards
Enter key	Run an action

Simple elements

Table 3: Overview of the controls used

Button	Use the Tab key to navigate to the control and press Enter to run the action.
Link	Navigate to the required link with Tab and press Enter to open a new page or

	dialog.
Dialog window	Click the Esc key to leave the dialog window without taking any action. Click Enter to run. If there is more than one action available, navigate to the desired action with the Tab key and press the Enter key.
Menu	Navigate to the menu using Tab. The selected element changes its color. Press Alt+ **Move down** or **Move up** to expand the entire menu. Use the arrow keys to choose between the different elements. Use Tab to leave the menu. You do not need to confirm by pressing Enter or Space.
Input field	Navigate to the desired field. If text input is possible, the cursor blinks and you can write in the field. Use Tab to exit the field. You do not need to confirm by pressing Enter or Space.
Tiles	Use the Tab key to navigate to the tile and press Enter to display the page's content.
Check box	Use the Tab key to navigate to the required check box and press Space to enable the check box.
Option	Use the Tab key to navigate to the required list of options. Use the arrow keys to choose between the different options. Use Tab to leave the list of options.

Installed controls

Table 4: Overview of other controls

Tree view	Use Enter to expand or collapse a tree view. A plus sign next to the tree means it can be expanded by pressing Enter. A minus sign means the element can be collapsed by pressing Enter.

Search

Many of the pages provide a function to search for objects in context. For example, if you view the your managed resources, you can search for a specific resource. You can select the simple search, where you enter a single search string, or the advanced search, where you can apply several parameter to the search.

TIP: The search does not take upper and lower case into account.

There are certain rules that enable a successful global search in the Web Portal. These are described in the following table using examples.

Table 5: Rules with examples for searching in the Web Portal

Example	Description
Sam User	Finds Sam User but not Sam Identity.

Example	Description
	Search results must contain all of the separate terms in the query. A logical **AND** is used.
Sam OR Identity	Finds Sam User and Pat Identity. Placing **OR** between the search terms acts as a logical OR operator. The results of this search contain at least one of the two search terms.
Sam NOT User	Finds Sam Identity but not Sam User. The results of this search do not contain the term that comes after **NOT**.
U*	Finds User1 and User2. The * functions as a wildcard for any number of characters to complete the term.
Use?	Finds User but not User1. The **?** functions as a wildcard for a single character to complete the term.
"Sam User"	Provides results in which the search terms **Sam** and **User** follow one another. Results of this search contain the string in quotes as phrase.
Sam User~	Finds Sam User and also other similar results. A tilde **~** after the search term indicates that the search should also find similar results. This means that incorrectly spelled terms can be found, as well. You can specify the level of similarity by adding a number between **0** and **1** (with decimal point) after the tilde **~**. The higher the number, the more similar the results.

Detailed information about this topic

- Running a search on page 35
- Context searching on page 36
- Advanced search on page 36

Running a search

Search is available at all times in the header.

To run a search

1. In the header, in the field next to 🔍, enter the search term.
2. Click 🔍 in the header.

   The **Search results** view opens, displaying all the results that match your query.

Context searching

A context search is context-dependent unlike a regular search, and is available where several entries are listed. For example, the **Request history** view normally lists several entries and a context search is available above the list.

To run a context search

1. In the field next to 🔍, enter the search term.
2. Click 🔍.

   Any results matching your query are displayed.

Advanced search

Advanced searching is context-dependent, like the context search, but offers various other additional search settings. The advanced search is often found next to the context search and can be opened with a link. You can use the advanced search in the **Request history** view, for example.

To run an advanced search

1. Click **Advanced search** in the view above the list.

   The following table lists the possible search settings.
2. Enable the relevant check boxes next to the criteria you would like to use to limit the search.
3. Click **Search**.

   Any results matching your query are displayed.

Sorting

A sort function is available to you for all tables.

To sort a table

1. Click in the column header you want to sort.

   You will see an icon to the right of the column name.
2. Click again in the column header to sort in ascending or descending alphabetical order.

   This sorts the column as required.
3. Click again in the column header to sort in the opposite order.

   This sorts the column as required.

To sort a table by several columns

You can select any column to sort by multiple columns. You can add another column by holding the Ctrl key and clicking with the mouse.

NOTE: The first column selected has the highest priority in the sort order. If you want to sort in a particular order, select this column last. All the columns selected before are included in the sort order.

Table 6: Multiple column sorting

Handling	Description
Select the first column.	Click in the column header.
Select more columns.	Click in the header whilst holding down the Ctrl key.
Sort in the opposite order.	Click again in the header whilst holding down the Ctrl key.
Cancel the sort order/Resort	Click in the header of any column to apply a new sort order.

Bookmarks

You sometimes have the option to set bookmarks in views in the Web Portal. Bookmarks have the advantage that you can use them to navigate straight to a particular part in the Web Portal when you log in again.

TIP: If you frequently request a particular service item from a service category, for example, you can navigate faster to this service category by setting a bookmark.

Detailed information about this topic

- Setting bookmarks on page 37
- Selecting bookmarks on page 38
- Deleting bookmarks on page 38

Setting bookmarks

MOBILE: This function is not available in the mobile interface.

To set a bookmark

1. Go to the page where you want to set the bookmark.
2. On the page, click (**Create bookmark**).

   The **Bookmark this page** link changes to **Remove bookmark**. The bookmark is displayed on the home page and in the header.

NOTE: Not every page in the Web Portal can be bookmarked.

Selecting bookmarks

To select a bookmark

1. Open the home page.
2. Perform one of the following tasks:
    - On the home page, in the **Bookmarks** tile, click the required bookmark.
    - In the header, click (**Bookmarks**) and click the required bookmark.

    This navigates to the page you have bookmarked.

Deleting bookmarks

If you there is bookmark that you no longer need, you can delete it from a view at anytime. You can also delete bookmarks on the page that the bookmark references.

To delete a bookmark

1. In the header, click (**Home**).
2. On the start page, click **Explore** in the **Bookmark** tile.
3. In the **Bookmark** dialog, click **Delete** next to the bookmark that you want to delete.
4. In the **Delete bookmark** prompt, confirm with **Yes**.

Help

You can find the help menu in the header bar Several menu items are shown when you select this menu.

Detailed information about this topic

- Using the help on page 39
- Support on page 39
- Community on page 39
- Connection on page 39
- Info on page 40

Using the help

You can use the guide as well as online help to answer questions about the Web Portal.

To call up help in the Web Portal

- In the header, click (**Help**) > **Documentation**.

Support

The support portal is there to give you technical support. There you can find a large number of solutions to different issues.

To open the support portal

- In the header, click **Help** > **Support**.

  The support portal opens.

Community

The One Identity Community offers you a forum where you can exchange information and solutions with other users.

To open the One Identity Community forum

- In the header, click **Help** > **Community**.

  This opens the One Identity Community forum.

Connection

You can to call up information about a database session and view it in the Web Portal.

NOTE: You cannot change any data in the database.

The data connection details are displayed in a dialog window. You can see information about the web application user, permissions groups and the program functions that are allowed.

Information about the user is shown in the **System user** view. Here, you will find out more about the authentication type, user ID, what permissions the user has (read and/or write access), whether the user is a dynamic user and how the user was added.

You can view permissions groups with a description about each group listed on the **Permissions group** view.

A list of program functions with a description is available on the **Program functions** view.

To open the "Connection" dialog.

1. In the header, click > **Connection**.
2. In **Connection**, click the tab corresponding to the type of information that you would like to view in more detail.

Info

The **About** menu shows you, among other things, information about your currently installed version of the Web Portal and the registered names of the product. It is displayed in dialog containing the following views.

- About

  Displays the registered trade mark names and the current version of the Web Portal installed.
- Legal Notices

  Lists components from third-parties included in the Web Portal. The contact data and the component license might also be given.
- Contact

  This shows the contact data for purchasing queries or other questions.

To open the "About" dialog

1. In the header, click **Help** > **About**.
2. Select the view for the information type you want to view in more detail.

Filtering

You can find the filter function represented by (**Filter**) in a lot of table columns. It provides you with a selection of different filters.

NOTE: The contents of the filters vary depending on context. You can filter by text, numeric values, fixed values, such as gender, "yes" or "no", dates, or objects.

MOBILE: This function is only available in the list view of the mobile interface.

To use a filter

1. Open a menu which shows tables.
2. Click on the required column.
3. Select the filter that you want to apply.
4. Click **Apply**.

Detailed information about this topic

- Text filters on page 41
- Number filters on page 41
- Object filter on page 42
- Filtering the calendar function on page 42
- Delete filter on page 43
- Custom filter conditions

Text filters

You can find a text filter in the **Product** column of the **Request History** view.

To apply filter criteria to text

1. Enter one or more terms in **Filter on...**.
2. Select one of the following criteria from the text filter's menu.

Table 7: Other criteria for applying text filters

Filter	Description
All words	This displays all search results, which contain the term in the field.
Starts with	Only results, which start with the given term are displayed.
Ends with	Only results, which end with the given term are displayed.
One or more words	Only results containing at least on of the given terms are displayed.

Number filters

You can find a number filter, for example, in the **Risk index** column in **High Risk Overview**.

To apply filter criteria to numerics

1. Enter a value in the field or use the arrow keys to set a number.
2. Select one of the following criteria from the numeric filter's menu.

Table 8: Other selection criteria for using numeric filters

Filter	Description
greater or equal	Only results with a value the same or higher than the given value are shown.
less or equal	Only results with a value the same or lower than the given value are shown.
Between	Only results with a value the between the given values are shown.

Object filter

You can find an example of an object filter in the **My Responsibilities** > **Identities** menu in the **Primary Department** column header.

To apply an object filter

1. In the **Filter on ...** dialog, select **Filter by object**.

   The results are shown by default in a hierarchical structure. Unselected objects are identified with .

   You can switch to list view using the icon and back again with .
2. Click the required object.

   The selected object is marked with and listed under **Selected**.

   NOTE: To deselect a selected object, click on the object in the details pane.
3. Click **Apply**.

   The filter is applied. The matching results are displayed in the view.

Filtering the calendar function

The "Calendar function" filter is, for example, available in the **Request date** column of the **Request History** view.

To apply filter criteria to the calendar function

1. Select one of the following criteria in the context menu next to the field.

Table 9: Other criteria for applying filters to the calendar function

Filter	Description
After	Only displays results after this date.
Before	Only displays results before this date.
Between	Only displays results between these dates. Another field with calendar icons is displayed with this setting.
This week	Only displays results with this week's date.
Last week	Only displays results with last week's date.
This month	Only displays results with this month's date.
This year	Only displays results with this year's date.

2. Perform one of the following tasks:
    - Click and select a date.
    - Enter the date in the field.
3. Click **Apply**.

    The filter is applied. The matching results are displayed in the view.

Delete filter

After setting a filter, you can remove it again manually or it is removed automatically when you change views.

To delete a filter

- Perform one of the following tasks:
    - Click in the filtered column.
    - Click in the row above the entire table.

Custom filter conditions

In some places in the Web Portal you can create custom filter conditions. The filter conditions are formulated like a condition (WHERE clause) for a database query.

You can use a wizard to formulate the queries. Each condition is displayed in a special control in the wizard.

The wizard is available to you at different places in the Web Portal.

To open the filter wizard

- Click **View settings** > **Open filter wizard**.

Detailed information about this topic

- Creating filters using the wizard on page 44
- Using control elements on page 47
- Displaying technical names of database columns on page 47
- Displaying filter conditions as SQL expressions on page 48

Creating filters using the wizard

To create a filter with the wizard, first select a column, edit the conditions and comparison operators. Once these settings have been configured, you can apply the filter.

To create and apply a filter with the wizard

1. Click **View settings** > **Open filter wizard**.
2. Select the column for the table in the filter wizard.
    a. Click **At least one entry exists** and specify whether the column should reference or be referenced from other tables.

    The following views are available.

Table 10: Views in the filter wizard

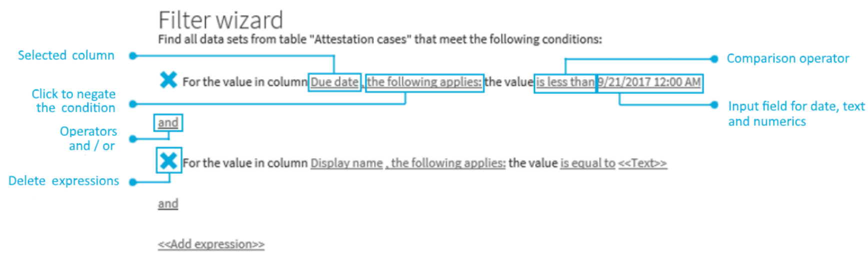
View	Description
Value comparison	Compares the values of the selected columns. These columns are part of the table you want to apply the custom filter to. The advantage of using the WHERE clause wizard is that you can select all the table's columns as opposed to the filter function, which only provides a default selection of columns.
References to other objects	Creates a n:1 relation. Select the desired table B in this view. Several data records from table A can be assigned to one data record in table B. A data record in table A cannot be assigned more than one data record from table B.
References for assignment tables	Creates a 1:n relation. Each data record in table A can be assigned to

View	Description
	several data records from table B and vice versa. These relations are realized through a third Table for realizing assignment tables Assignment table only contains the foreign keys of the other tables A and B.
References from other objects	Creates a 1:n relation. Select the desired table B in this view. Several data records from table B can be assigned to one data record in table A. A data record from table B cannot be assigned to more than one data record from table A.

b. Select the desired column in the **Filter wizard** view.

This inserts a control for the first condition.

Figure 1: Filter wizard with example conditions



3. Enter the condition and configure the following settings:
   a. Enter the comparison value.

      You can enter a date, numeric, or text value. The input of the value type depends on the selected column.
   b. Change the comparison operator.

      To change the comparison operator, click the comparison operator "is less than", for example.

      The type of comparison operator depends on the column type. The following comparison operators are available.

Table 11: Comparison operators

Value type	operator	Description
Text value	is equal to	Finds the same text value.
	Precedes the word in the alphabet	Finds all results that occur before the entered text in alphabetical order.
	Follows the word in the alphabet	Finds all results that occur after the entered text in alphabetical order.
	Not equal	Finds all results that are not the same as the entered text.
	Is contained in	Finds all results that contain the text value.
	Contains	Finds all results that contain the text value.
	Begins with	Finds all results that begin with the entered text value.
	Ends with	Finds all results that end with the entered text value.
	Is equal or precedes the word in the alphabet	Finds all results that either contain the entered text value or occur before the entered text value in alphabetical order.
	Is equal or follows the word in the alphabet	Finds all results that either contain the entered text value or occur after the entered text value in alphabetical order.
Numerical value	Is less than	Finds all results that are smaller than the entered numerical value.
	Is greater than	Finds all results that are larger than the entered numerical value.
	is equal to	Finds all results that are the same as the entered numerical value.
	Is less or equal	Finds all results that are less than or equal to the entered numerical value.
	Is greater than or equal	Finds all results that are greater than or equal to the entered numerical value.
	Not equal	Finds all results that are not the same as the entered numerical value.

c. Change the Boolean value if the option is available in the selected column.

   The value **false** is selected by default. If you change the value to **true**, data appears that matches the content of this column.

d. To negate the defined condition, click **applies**.

   The condition statement is reversed and the data displayed after filtering, does not match this condition. This setting is not available if the Boolean option can be set.

e. Use the operators and or or when applying multiple conditions.

   NOTE: Remove the control by clicking .

4. Insert another expression with **<<Add expression>>** and repeat this step if required.
5. Perform one of the following tasks:
   - Apply the filter by clicking **Apply**.

     This returns you to the original view where a message alerts you to the active filter wizard.

   - Close the wizard with **Close**.

Using control elements

The filter wizard view can quickly become confusing if several conditions are used with different controls. In this case, you can expand or collapse the conditions with your controls.

To expand or collapse controls.

1. Click **View settings** > **Open filter wizard**.
2. Perform one of the following tasks:
   - Click **Collapse all** in the **Filter wizard**.
   - Click **Expand all** if the controls are collapsed.

Displaying technical names of database columns

You can display the technical names of database columns instead of the display names.

To display technical names of database columns

1. Click **View settings** > **Open filter wizard**.
2. Click **Show technical name**.

   This displays all the table and column names that occur in the filter wizard with their technical names.

3. If you would like to view the table and column display names again, click **Show display**.

Displaying filter conditions as SQL expressions

In the expert view you can view and edit filter conditions as SQL expressions.

To view a custom filter condition as SQL expression or to write one manually

NOTE: To open the expert view, you must own the role of administrator, auditor, or compliance & security officer.

1. Click **View settings** > **Open filter wizard**.
2. Click **Expert mode**.

   If you have already created a filter, the filter condition is shown in the SQL editor as an SQL expression.
3. Perform one of the following tasks:
   - Edit the SQL expression in the field.
   - Enter the SQL expression in the field.
4. Click **Apply**.

   Applies the filter.

Grouping and ungrouping columns

Grouping is offered for views with a large number of entries. You can group columns in the **Auditing** view on the **Attestation policy** column, for example.

MOBILE: This function is only available in the list view of the mobile interface.

To group by column or ungroup

1. Select the filter in the column you want and click **Group by this column**.

   The entries are displayed in groups.
2. Open the group with >.

   This displays all the entries in the group.

   - OR -
3. Delete the filter.

   This dissolves the group.

Showing other columns

You can blend in other columns you want to see in your view.

MOBILE: This function is only available in the list view of the mobile interface.

To include other columns in the table

1. Click **View settings** > **Additional columns**.

   This opens **Additional columns**.
2. Enable the check box next to the column you wish to display.
3. Click **Apply**.

   Now you can see the selected columns in the table and use them.

Saving views

If you have modified a view and think you might want to use it at a later date, you can save the view settings.

NOTE: The saved view is only available at the location where you saved it.

To save the current view

1. Click **View Settings** > **Save current view**.

   This opens the **Save current view** dialog.
2. Enter a name for the view in the field.
3. Click **Save**.

TIP: You can select and apply the saved view at any time under **View settings**.

Deleting saved views

You can delete saved views in view settings.

NOTE: The saved view is only available at the location where you saved it.

To delete a saved view

1. Click **View settings** > **Edit list**.

   This opens the dialog **Edit view settings**.
2. Click 🗑 after the view setting that you want to delete.

   The deleted view setting is removed from the dialog and you cannot select it in the menu anymore.

Exporting views

You can save a view in PDF or CSV format, or as a website for use as a report. This function is available at different points in your web application. For more information, see Exporting

reports on page 68.

NOTE: You cannot export more than 100 000 data sets. If there are more data set, only the first 100 000 are exported.

To export a view

1. Click **View settings** > **Export this view**.

   This opens the dialog **Export this view**.

2. Select one of the following options:
   - **Export as PDF**: exports the view as a PDF file.
   - **Export as CSV**: exports the view as a CSV file.
   - **Display as website**: exports the view as a report in HTML format.

3. (Optional) Enable the following check boxes:
   - **All pages**: All pages of the view were exported. If this setting is not enabled, only the current page is exported.
   - **Remove header**: Removes the first row of the table. This row contains the column names.

     NOTE: This setting is only available if you selected the option **Export as CSV** in the previous step.

4. Click **Export**.

   Exports the view.

Mobile view

The Web Portal is designed for use with desktops computers and mobile devices. The views are adjusted automatically. In the mobile view, some functions are limited or not at available at all.

Table 12: Handling options for mobiles

Action	Handling
Open menu bar	The menu that you find horizontally under the header in the desktop version is opened on mobile devices as follows: 1. Press ☰ . List lists the menus under each other. 2. Press > next to a menu. This displays other menu items.
Display extended functions/header	You open the functions and settings in the header toolbar (such as search) for mobile devices as follows:

Action	Handling
	1. Press ⋮ . Menus are displayed next to each other. 2. Press on one of the following icons: • : Opens search. • : Contains the menus **My profile**, **My settings**, **Telephone book**, and **Log off**. • : Opens your shopping cart without requests. • : Shows any saved bookmarks. NOTE: Replace this text with a description of a feature that is noteworthy. • : Contains the menus **Help**, **Support**, **Community**, **Connection** and **Info**.

Heatmaps and statistics in the mobile view

The following handling options apply for heatmaps and statistics in the mobile view.

Table 13: Handling options for heatmaps and statistics

Action	Handling
Show tooltip	Tap on the statistic or the diagram.
Display more details about the statistic/diagram in the dialog	Double-tap on the statistic or the diagram.
Display a tooltip for a heatmap rectangle	Tap the heatmap's rectangle.
Zoom in on heatmap	Double-tap on the heatmap.

Displaying the address book

If you need information about an identity such as the phone number or location, you can use the address book. This gives a quick overview of an identity and further details.

To display the address book

1. In the header, click **(Profile)** > **Address Book**.

   This displays the address book and all identities (see Address book on page 851).

2. (Optional) On the **Address Book** page, click an identity.

   For more information, see the details pane.

3. (Optional) In the details pane, click **Overview**.

   This opens the identity's overview page. Here you can gather further information about the identity (for example, main data, requests, entitlements, and so on). For more information, see Displaying my identities' overviews on page 303.

Related topics

- Address book on page 851
- Displaying my identities' overviews on page 303

Managing password questions

If you forget your password, you can change it at any time in the Web Portal (see Changing passwords on page 55). To do this, you need to define individual questions that only you can answer.

If your password questions are answered incorrectly several times, they may be locked (depending on the system configuration). You can reset locked password questions at any time.

TIP: Once a password question is locked because you answered it incorrectly, you will be asked to answer another password question. This is repeated until there are not enough (unlocked) password questions left. To be on the safe side, make sure you create enough password questions.

If the Web Portal is configured accordingly, password questions are deleted after successful use.

Detailed information about this topic

- Creating password questions on page 53
- Editing password questions on page 53
- To unlock password questions on page 54
- Deleting password questions on page 54

Creating password questions

You can create new password questions.

To create new a password question

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click the **Password** tile.
3. On the **Password Questions** page, click **New question**.
4. In the **New password question** dialog, enter the following:
   - **Secret question**: Enter your question.
   - **Secret Answer**: Enter the answer to your question (above).
   - **Confirm secret answer**: Enter the answer to your question again.
5. Click **Apply**.
6. On the **Password Questions** page, click **Save**.

Related topics

- My profile (page description) on page 847
- Password questions (page description) on page 850

Editing password questions

You can edit existing password questions.

To edit a password question

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click the **Password** tile.
3. On the **Password Questions** page, click **Edit** next to the password question you want to edit.
4. In the **Password question** dialog, enter the following:
   - **Secret question**: Enter your question.
   - **Secret Answer**: Enter the answer to your question (above).
   - **Confirm secret answer**: Enter the answer to your question again.
5. Click **Apply**.
6. On the **Password Questions** page, click **Save**.

Related topics

- My profile (page description) on page 847
- Password questions (page description) on page 850

To unlock password questions

You can unlock locked password questions to reuse them again.

TIP: On the **Password Questions** page, locked password questions are labeled with **(locked)**.

To unlock a password question

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click the **Password** tile.
3. On the **Password Questions** page, next to the password question you want to unlock, click **Edit**.
4. In the **Unlock password question** dialog, confirm the prompt with **Yes**.
5. On the **Password Questions** page, click **Save**.

Related topics

- My profile (page description) on page 847
- Password questions (page description) on page 850

Deleting password questions

You can delete existing password questions.

To delete a password question

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click the **Password** tile.
3. On the **Password questions** page, next to the password question you want to delete, click **Edit**.
4. In the **Password question** dialog, click **Delete**.
5. In the **Delete password question** dialog, confirm the prompt with **Yes**.
6. On the **Password Questions** page, click **Save**.

Related topics

- My profile (page description) on page 847
- Password questions (page description) on page 850

Changing passwords

You can use the Password Reset Portal to change your central password or change multiple passwords for various user accounts.

You can change your password(s) in a few steps:

1. Log in to the Password Reset Portal.
2. Change the relevant password(s).

Step 1: Log in to the Password Reset Portal

Log in to the Password Reset Portal using a passcode, by answering your password questions, or with your current password (see Logging in to the Password Reset Portal on page 30).

Step 2: Change password

After you have logged in on the Password Reset Portal (see Step 1: Log in to the Password Reset Portal on page 55), you can change your central password or the passwords of user accounts to which you have access.

To assign a new password for your personal user account or another user account

1. On the **Manage My Passwords** page, select the option **I want to reset one or more passwords**.
2. Perform one of the following tasks:
   - To change the passwords for your personal user accounts, next to **Personal accounts**, click ▶ **Expand**.
   - To change the passwords of other user accounts, next to **Other accounts**, click ▶ **Expand**.
3. Select the check box next to the user accounts whose passwords you want to change.
4. Click **Next**.
5. On the **Set a new password** page, enter the password you wish to use in the **New password** field.

   TIP: Below the field, you can see how secure your new password is.
   To display your company's password specifications, click **Password policy**.
6. In the **Repeat the password** field, enter the password again.

7. Click **Next**.

   The password is reset for the previously selected user accounts.
8. On the **Success** page, click **Log off**.

To change the central password

1. On the **Manage my passwords** page, select the option **I want to reset my central password**.
2. Click **Next**.
3. On the **Set a new password** page, enter the password you wish to use in the **New password** field.

   > TIP: Below the field, you can see how secure your new password is.
   > To display your company's password specifications, click **Password policy**.
4. In the **Repeat the password** field, enter the password again.
5. Click **Next**.

   The central password is reset.
6. On the **Success** page, click **Log off**.

Related topics

- Managing password questions on page 52

Unlocking user accounts

Your account might be locked for use if, for example, you (or an unauthorized person) have tried to log in too many times using the wrong credentials.

You can unlock your user account in two steps:

1. Log in to the Password Reset Portal using a passcode. You obtain the passcode from your manager.
2. Enter a new password.

   You will then be able to use your user account again.

Related topics

- Logging in to the Password Reset Portal on page 30
- Changing passwords on page 55

Editing your profile information

You can update your contact information at any time.

NOTE: You cannot edit light gray boxes.

To update your contact information

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click **Contact data**.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.

   NOTE: Changes to your contact data only affects the selected identity.
4. Edit the entries in the various fields.
5. (Optional) To change your profile picture, perform the following actions:
   a. Click (**Change**) next to **Picture**.
   b. In the **Picture** dialog box, click **Choose File**
   c. Select an image from your medium.

      NOTE: If the photo is greater than 10 KB, you will have to crop the image. To do this, hover the mouse cursor over the selected photo until a crosshair appears, click the left mouse button and drag the mouse over the image until the desired area is selected, click **Crop to selection**, and then click **Apply**.
6. Click **Save**.

Editing Active Directory user accounts

You can edit your Active Directory user accounts at any time once you have logged in to the system and the user data has loaded.

NOTE: This function is only available if Active Roles Module is installed. This module references Active Roles extensions in Active Directory user accounts.

To edit your Active Directory user accounts

1. In the header, click (**Profile**) > **My Profile**.
2. On the **Overview** page, click **Active Directory user accounts**.
3. Enable the required Active Directory user account, if several are available.
4. Edit the fields or add new ones.
5. Save the changes.

Switching languages

In the Web Portal, you can specify which language you want to use for the Web Portal.

NOTE: If you have not explicitly assigned a language in the Web Portal, the language used by your browser will be adopted.

To change the language of the Web Portal

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click **Contact data**.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Contact Data** page, next to the **Language** field, click **Assign** or **Change**.
5. In the **Language** dialog, select the language that you want to use for the Web Portal.
6. On the **Contact Data** page, click **Assign** or **Change** next to the **Language for value formatting** field.
7. In the **Language for value formatting** dialog, select the language you want to use for date and number formats.

   For example, German dates are displayed in the format DD.MM.JJJJ (**24.12.2020**) and in English US format MM/DD/JJJJ (**12/24/2020**).
8. On the **Contact data** page, click **Save**.

   The changes will take effect as soon as you call a new page or refresh the page.

TIP: You can also change the session language by clicking **Help** > **Language** in the header.

Enabling/disabling email notifications

You can define which events you would like to be notified about by email.

To enable/disable email notifications

1. In the menu bar, click **Settings**.
2. On the **My Settings** page, click the **Email Notifications** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Email Notifications** tab, perform one of the following actions:
   - To enable notifications, select the check box **Notify me** next to the event that you want to notified about.

- To disable notifications, deselect the box **Notify me** next to the event that you do not want to notified about any longer.

5. Click **Save**.

Personal dashboard settings

In**Personal Dashboard Settings**, you can hide or show dashboards with neutral trends. Dashboards with "neutral trends" are those that have not change recently. By default, this filter is not enabled. You can also hide other dashboards. To hide individual dashboard, you can use the filter function on the desired dashboard view. For more information, see Hiding statistics on page 797.

To show a dashboard

1. Open **Personal Dashboard Settings**.
2. Perform one of the following tasks.
    a. Enable **Show dashboards with neutral trends**.
    b. Select one of the displayed statistics that you want to display again.
3. Click **Save**.

Report subscriptions management

Web Portal provides several reports that present information about objects and their relations to other objects in the database. Identification, analysis, and summaries of relevant data are supported with the help of these reports.

You can subscribe to reports in the Web Portal in order to receive them on a regular basis. These subscriptions can be managed by you.

For more information about report subscriptions, see the *One Identity Manager Report Subscriptions Administration Guide*.

Detailed information about this topic

- Subscribing to reports on page 60
- Editing report subscriptions on page 60
- Sending reports from report subscriptions on page 61
- Unsubscribing reports on page 62
- Reports on page 62

Subscribing to reports

You can subscribe to reports. These reports are regularly sent by email to you and any other subscribers.

To add a subscription

1. In the menu bar, click **Settings**.
2. On the **My Settings** page, click the **Subscriptions** tab.
3. In the **My Subscriptions** pane, click **Add subscription**.
4. In the **Add report subscription** dialog, in the list, click the report that you want to subscribe to.
5. Click **Next**.
6. In the **Edit report parameters** step, specify the following subscription settings:
   - **Subscription**: Enter the subscription's name.
   - **Schedule**: Select how often you want to receive the report (once a week, for example).
   - **Format (email attachment)**: Select which format you want to receive the report in. The report is sent in this format as a file attachment in an email.
   - (Optional) Specify other report specific settings. These settings might vary depending on what report you use.
7. Click **Next**.
8. In the **Additional subscribers** step, in the list, click the identities that will also receive this report.

   TIP: To remove a subscriber, in the **Current** list, click the corresponding identity.
9. Click **Save**.
10. In the **Overview** step, check your data.
11. Click **Close**.

Related topics

- Reports on page 62

Editing report subscriptions

You can edit your existing report subscriptions.

To edit a report subscription

1. In the menu bar, click **Settings**.
2. On the **My Settings** page, click the **Subscriptions** tab.
3. In the **My Subscriptions** pane, in the list, click the report subscription that you want to edit.
4. In the details pane, click **Edit**.
5. In the **Edit subscription settings** dialog, edit the following report subscription settings:
   - **Subscription**: Enter the report subscription's name.
   - **Report**: Select the report that you want to subscribe to.
   - **Schedule**: Select how often you want to receive the report (once a week, for example).
   - **Format (email attachment)**: Select which format you want to receive the report in. The report is sent in this format as a file attachment in an email.
6. (Optional) Specify other report specific settings. These settings might vary depending on what report you use.
7. Click **Save**.
8. On the **My Settings** page, in the report subscription's details pane, click (**Add identities to this subscription**).
9. In the **Additional Subscriptions** dialog, in the list, click the identity that should also receive the report.

   TIP: To remove a subscription, in the **Current** list, click the corresponding identity.
10. Click **Save**.

Related topics

- Reports on page 62

Sending reports from report subscriptions

Depending on how the schedule is configured, you can send reports to yourself and to others.

To send a report

1. In the menu bar, click **Settings**.
2. On the **My Settings** page, click the **Subscriptions** tab.
3. In the **My Subscriptions** pane, click the subscription in the list that you want to send.
4. In the details pane, click **Actions** > **Get report now**.

Related topics

- Reports on page 62

Unsubscribing reports

You can unsubscribe reports.

To unsubscribe a report

1. In the menu bar, click **Settings**.
2. On the **My Settings** page, click the **Subscriptions** tab.
3. In the **My Subscriptions** pane, in the list, click the report subscription that you want to edit.
4. In the details pane, click **Unsubscribe**.
5. In the dialog, confirm the prompt with **Yes**.

Related topics

- Reports on page 62

Reports

Reports contain information about objects and their relations to other database objects. Identification, analysis, and summaries of relevant data are supported with the help of these reports.

You can display, create, and edit reports. You and other Web Portal users can subscribe to these reports.

Detailed information about this topic

- Generating reports on page 63
- Editing reports
- Displaying report definitions on page 66
- Generating reports on page 68
- Exporting reports on page 68
- Report subscriptions management

Generating reports

In the default installation there are predefined reports available that you can subscribe to in the Web Portal. You can also create your own reports.

To generate a report

1. In the menu bar, click **Settings**.
2. On the **My Settings** page, click the **Reports** tab.
3. On the **Reports** tab, click **New report**
4. On the **Create a new report** page, enter the new report's main data.

Table 14: Report main data

Property	Description
Name	Enter the report's name.
Description	Enter a description for the report.
Risk index	Use the slider to define the report's risk index.
Disabled	Select the check box if the report cannot inherited by identities. Only subscribable reports that are enabled can be assigned within One Identity Manager. If a report is disabled, you are prevented from assigning the subscribable report. Existing assignments remain intact. IMPORTANT: If you disable a subscribable report, existing Web Portal user report subscriptions are canceled.
Owners	Click **Change** and select the identity responsible for this report. This identity can view and edit the report.
Report defin-ition	Click **Assign** and select the base table whose content you want to include in the report. Use **Columns** and **Edit filters** to specify which data should be included in the report.
Service item	Select a service item. To create a new service item, click **Create a new service item** and then create a new service item. The report can be requested through the service item.
Assign to identities	Click **Assign/Change** and select the identities that will receive the report.
Assign to departments	Click **Assign/Change** and select the departments that will receive the report.

Property	Description
Assign to Locations	Click **Assign**/**Change** and select the locations that will receive the report.
Assign to cost centers	Click **Assign**/**Change** and select the cost centers that will receive the report.

5. Click **Save**.

Editing reports

You can edit your own reports.

To edit a report

1. In the menu bar, click **Settings**.
2. On the **My Settings** page, click the **Reports** tab.
3. On the **Reports** tab, click the report you want to edit.
4. In the details pane, click **Show report definition**.
5. On the new page, click the **Main data** tab.

6. On the **Main data** tab, edit the report's main data.

Table 15: Report main data

Property	Description
Name	Enter the report's name.
Description	Enter a description for the report.
Risk index	Use the slider to define the report's risk index.
Disabled	Select the check box if the report cannot inherited by identities. Only subscribable reports that are enabled can be assigned within One Identity Manager. If a report is disabled, you are prevented from assigning the subscribable report. Existing assignments remain intact. IMPORTANT: If you disable a subscribable report, existing Web Portal user report subscriptions are canceled.
Owners	Click **Change** and select the identity responsible for this report. This identity can view and edit the report.
Report definition	Click **Assign** and select the base table whose content you want to include in the report. Use **Columns** and **Edit filters** to specify which data should be included in the report.
Service item	Select a service item. To create a new service item, click **Create a new service item** and then create a new service item. The report can be requested through the service item.
Assign to identities	Click **Assign**/**Change** and select the identities that will receive the report.
Assign to departments	Click **Assign**/**Change** and select the departments that will receive the report.
Assign to Locations	Click **Assign**/**Change** and select the locations that will receive the report.
Assign to cost centers	Click **Assign**/**Change** and select the cost centers that will receive the report.

7. Click **Save**.

Displaying report definitions

Use **View report definition** to view more information about an existing report and make changes if required.

- Overview

  View assigned properties of the selected report in a Hyper View.
- Main data

  Edit and modify report properties.
- Usage

  Viewing identity assignments to a role class.

Detailed information about this topic

- Overview on page 66
- Main data on page 66
- Usage on page 68

Overview

Using the **Show report definition** action, you can open, among other things, an overview of the selected report. All relevant information about the report is provided in abbreviated form in the overview, such as, assigned identities or application roles. They are displayed in shape elements.

To view a report's overview

1. Open **Reports** and select the report you want to view.
2. Click **Show report definition**.
3. Select **Overview** to view all the information about an identity at a glance.

Main data

Use **View report definition** to open the main data to add missing properties or to edit properties such as the risk index.

To edit the main data

1. Open the **Settings** menu and click **Reports**.
2. Select a report and, in the details pane, click **View report definition**.
3. Select **Main data** and edit the following settings.

NOTE: Any fields that are not marked with an asterisk (*) are optional. Optional fields can be filled in when you create the application or at a later stage.

Table 16: Report main data

Setting	Description
Name*	Field for the report name. Enter the report's name.
Report definition	Base table selection. Use **Change** to select the base table you want from a list.
Risk index	Display a scale of 0 to 1 for the risk index and two slide rulers. Specify a beginning and an end value within the scale.
Owner	Name of the report owner. Use **Change** to select from a list of owners.
Service item	Creating a new service item. Use **Create a new service item** to create a new product. You can disable this report definition using **Disable**.
Assign to identities	Selection of identities to receive the report. Use **Change** to select an identity to receive the report.
Assign to departments	Selection of departments to receive the report. Use **Assign** to select a department to receive the report.
Assign to Locations	Selection of locations to receive the report. Use **Assign** to select a location to receive the report.
Assign to cost centers	Selection of cost centers to receive the report. Use **Assign** to select a cost center to receive the report.

4. Click **Save**.

Usage

Use the **View report definition** function to display identity assignments to a role class in the **Usage** view.

To view which roles are contained in a predefined report

1. Mark a report in **Reports** view and click **View report definition**.
2. Select the **Usage** view.
3. Select a role class in the **Role classes** menu to see the roles contained in the report.
4. Select **More information** to view identities assigned to the role memberships.

Generating reports

You can generate reports and display the collected data.

To generate a report

1. In the menu bar, click **Settings**.
2. On the **My Settings** page, click the **Reports** tab.
3. On the **Reports** tab, click the report you want to display.
4. In the details pane, click **Show report**.

Exporting reports

Reports can help you to make necessary decisions. For example, when you are viewing your file system or SharePoint resources, you can view reports to help determine ownership. Or when you are performing attestations, you can view current information on the item to which you are attesting.

To export a report

1. In the menu bar, click **Settings**.
2. On the **My Settings** page, click the **Reports** tab.
3. On the **Reports** tab, click the report you want to export.
4. In the details pane, click **Show report**.

   This displays the report as a table in the view. There are filters for the columns in order to limit the display.

   NOTE: Before you export a view, you can add more columns to it.

5. Click **View Settings** > **Export this view**.
6. In the **Export this view** dialog, set the following as required.

All pages	All pages of the view were exported. If this setting is not enabled, only the current page is exported.
Remove header row	Headers are not included in the exported CSV file. This setting is only available for CSV format.

7. Perform one of the following tasks:
   a. To export a report as a PDF, enable the **Export as PDF** option.
   b. To export a report as a CSV file, enable the **Export as CSV** option.
   c. To export a report as a HTML file, enable the **Show as web page** option.
8. Click **Export**.

The user interface layout

The Web Portal user interface is divided into several sections:

Top - header

The header with the company logo is at the top of the screen. You can use different functions and reach different sections from here.

Top – menu bar

The menu bar is displayed horizontally in the upper part of the screen and provides different menus and submenus. To reach the Home page, click **Home**.

On the top right-hand side of the screen, select (**Settings**) to access the **My Settings** view. This page contains other options that you can use to configure your email notification and report settings.

Work area

The work area changes depending on the menu you opened from the navigation.

Detailed information about this topic

- Home on page 70
- Header on page 70
- Menu bar on page 71

Home

Open the home page with (**Home**).

Once you have logged in successfully, the home page appears. Displayed across the home page, there are tiles of different sizes that you can click on. The tiles allow you to access some frequently used menu items or important actions with one click.

Other tiles show statistics or heatmaps. You can also call up this information in full screen mode by clicking the relevant button.

Header

There are several buttons available to you in the Web Portal's header bar that make it easier and simpler to access functions and settings. The following table explains, which icons to select to reach the relevant functions and settings.

Table 17: Functions in the header

Search	The search helps you to search for various objects. For example, you can quickly and simply search for identities, attestation cases, or request procedures. For more information, see Search on page 34 and Running a search on page 35.
Inform-ation	Use these menu items to view: • Pending requests • Request inquiries • Pending attestations • Attestation inquiries • Pending rule violations • Pending policy violations and edit them. TIP: The moment this icon goes orange ( ), you have tasks pending.
My requests	Use these menu items to view: • Trigger new requests • Show and manage your shopping cart • Renew and cancel products TIP: The moment this icon goes orange ( ), the products are in your shopping cart.
Profile	Use these menu items to:

		• View your personal data with memberships, responsibilities, and entitlements and to edit setting (for example, your Password questions) • Display your company's address book • Log off • Change the language • Enable/disable email notifications • Manage report subscriptions
	Bookmarks	Show and select your bookmarks here. This icon is only shown if you have saved bookmarks in the Web Portal.
	Help	This menu includes online help, contact to customer service, community links, information about your connection and the product. Use **Help** to open the context-sensitive help. The help contains the entire contents of the Web Portal User Guide. **Connection** opens a dialog with detailed information about your web application connection. The information is divided out on **System users**, **Permissions groups**, and **Program functions**.

Menu bar

The menu bar is displayed horizontally in the upper part of the screen and provides different menus and submenus.

Menus are structured by topic. Each menu corresponds to a topic and holds further menu items that are respective subtopics.

To open a menu

1. In the menu bar, mouse-over a menu.

   This expands the menu and shows more menu items.

2. Click a menu item.

Table 18: Menus in the menu bar

Menu	Menu item	Actions
Request		
	My requests	• Start new requests • Show your request history • Renew and cancel products

Menu	Menu item	Actions
		• Cancel requests • Edit templates • Show and manage shopping carts
	My actions	• Manage pending requests • Show the approval history • Manage request inquiries
	Auditing	• Display requests of other identities • Show approvals
	Escalation	• Edit escalate requests
Attestation		
	My attestation status	• Show your pending attestation cases • Send reminder emails to attestors
	My actions	• Show and edit pending attestations • Show the attestation history • Show attestation inquiries
	Auditing	• Show all attestation cases
	Governance administration	• Show attestation runs • Manage attestation policies
	Escalation	• Show escalated attestations
Compliance		
	My actions	• Show and approve pending rule violations • Show historical rule violations • Show and edit pending policy violations • Show historical policy violations
	Auditing	• Show rule violations • Show policy violations
	Governance Administration	• Show and edit risk index functions • Show compliance information • Show critical object overview

Menu	Menu item	Actions
		• Show compliance rules and rule violations • Show company policies and policy violations • Show compliance rules with SAP functions and respective rule violations • Show compliance rules with SAP functions and respective rule violations • Show compliance rule violations of identities with critical SAP functions
Responsibilities		
	My responsibilities	• Show and manage the identities you are responsible for • Show and manage system entitlements • Show and manage business roles • Show and manage system roles • Show and manage departments • Show and manage cost centers • Show and manage locations • Show and manage application roles • Show and manage resources • Show and manage assignment resources • Show and manage multi-request resources • Show and manage multi requestable/unsubscribable resources • Show and manage software • Show and manage devices
	Delegation	• Show, create, and delete delegations • Show delegation history
	Responsibilities	• Add ownerships • Assign owners to system entitlements and devices
	Auditing	• Audit identities • Audit business roles

Menu	Menu item	Actions
		• Audit system roles • Audit application roles • Audit departments • Audit cost centers • Audit locations • Audit resources • Audit assignment resources • Audit multi-request resources • Audit multi requestable/unsubscribable resources • Audit software • Audit (Azure Active Directory, LDAP, SAP R/3, Universal Cloud Interface, UNIX)
	Governance Administration	• Show and manage the company structure (organization) • Show and manage identities and their entitlements • Show and edit business roles • Show and manage system entitlements
Calls		
	New Call	• Create calls
	Call history	• Show call history • Remove call attachments
Applications		Call stored application

Security keys (WebAuthn)

To open the **Security key** page, go to > **My profile** > **Security keys** (see Displaying security keys on page 76).

One Identity offers you the option to log in, simply and securely, to One Identity Manager web applications with help of (physical) security keys. If your system is configured for it and you own security keys like this, you must use the security key when you enter your password to log in to a web application (for example, to the Web Portal). These security keys support the W3C standard **WebAuthn**.

IMPORTANT: The WebAuthn standard is NOT support in Internet Explorer. Therefore, use another browser if you want to log in to One Identity Manager web application using security keys.

For more information about how you log in to the Web Portal with the help of security keys, see Logging in with security keys on page 30.

If you loose your security key or you cannot use it for any other reason, you can set up a new one using a passcode in the Password Reset Portal (see Setting up security keys on page 77).

On the **Security keys** page, view your security keys, set up new security keys, edit security keys and delete security keys.

The following tables give you an overview of the various functions and contents of the **Security Keys** page.

Table 19: Security keys

Column	Description
Registered	Shows you the date on which the key was registered.
Last used	Shows you the date on which the security key was last used.
Times used	Shows you how often the security key has been used.

Table 20: Controls

Control	Description
Edit	Use this button, to edit the respective security key.

Control	Description
Delete	Use this button to delete the respective security key.
New security key	Use this button to set up a new security key.

Detailed information about this topic

- Logging in with security keys on page 30
- Displaying security keys on page 76
- Setting up security keys on page 77
- Editing security keys on page 77
- Deleting security keys on page 78

Displaying security keys

You can display your security keys at any time.

To display your security keys in the Web Portal

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click the **Security keys** tile.

   This opens the **Security keys** page and shows you your security keys and details.

To display your security keys in the Password Reset Portal

1. Log in to the Password Reset Portal (see Logging in to the Password Reset Portal on page 30).
2. On the **Manage my passwords** page, select the **I want to manage my security keys** option.

   This will display your security keys and details.

Related topics

- Security keys (WebAuthn) on page 75
- Setting up security keys on page 77
- Editing security keys on page 77
- Deleting security keys on page 78

Setting up security keys

You can set up or register new security keys at anytime.

NOTE: To set up a security key, you require a physical key that you can connect to your computer by USB or NFC, for example.

To set up a security key in the Web Portal

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click the **Security keys** tile.
3. On the **Security keys** page, click **New security key**.
4. Follow the instructions.

   This sets up the security key. On the Security keys page, you can **edit** the security key at anytime.

To set up a security key in the Password Reset Portal

1. Log in to the Password Reset Portal (see Logging in to the Password Reset Portal on page 30).

   TIP: If you loose your security key or you cannot use it for any other reason, you can set up a new one using a passcode in the Password Reset Portal. To do this, you must ask your manager for a passcode and use it to log in to the Password Reset Portal.
2. On the **Manage my passwords** page, select the **I want to manage my security keys** option.
3. Click **New security key**.
4. Follow the instructions.

   This sets up the security key. You can edit the security key at anytime.

Related topics

- Security keys (WebAuthn) on page 75
- Displaying security keys on page 76
- Editing security keys on page 77
- Deleting security keys on page 78

Editing security keys

You can edit security keys at anytime.

To edit a security key in the Web Portal

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click the **Security keys** tile.
3. On the **Security keys** page, under the security keys you want to edit, click **Edit**.
4. In the **Edit security key** dialog, in the **Display name** field, enter a name for the security key.
5. Click **Save**.

To edit a security key in the Password Reset Portal

1. Log in to the Password Reset Portal (see Logging in to the Password Reset Portal on page 30).
2. On the **Manage my passwords** page, select the **I want to manage my security keys** option.
3. Under the security keys you want to edit, click **Edit**.
4. In the **Edit security key** dialog, in the **Display name** field, enter a name for the security key.
5. Click **Save**.

Related topics

- Security keys (WebAuthn) on page 75
- Displaying security keys on page 76
- Setting up security keys on page 77
- Deleting security keys on page 78

Deleting security keys

If you no longer need your security key or you have lost it, you can delete it at anytime.

NOTE: If you only have one key left, you cannot delete it. You last security key can only be deleted by an employee administrator. For more information about how to delete WebAuthn security keys as an employee administrator, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To delete a security key in the Web Portal

1. In the header, click (**Profile**) > **My profile**.
2. On the **Overview** page, click the **Security keys** tile.
3. On the **Security keys** page, under the security keys you want to delete, click **Delete**.
4. In the **Security key** dialog, confirm the prompt with **Yes**.

To delete a security key in the Password Reset Portal

1. Log in to the Password Reset Portal (see Logging in to the Password Reset Portal on page 30).
2. On the **Manage my passwords** page, select the **I want to manage my security keys** option.
3. Under the security keys you want to delete, click **Delete**.
4. In the **Security key** dialog, confirm the prompt with **Yes**.

Related topics

- Security keys (WebAuthn) on page 75
- Displaying security keys on page 76
- Setting up security keys on page 77
- Editing security keys on page 77

3

Requests

Requests account for the core functionality of the Web Portal. For example, if you require access to a system or device, request it as though you were using a traditional web shop. For more information about the **Request** menu and its menu items, see Request (Menu description) on page 852.

NOTE: You can request a variety of products depending on the entitlements assigned to you.

You can apply the following requests:

- Groups (for example, Active Directory groups, Notes groups, LDAP groups, and more)
- Membership in roles (for example, business roles, departments, application roles, applications, and more)
- Access to file systems or SharePoint resources
- Every other resource in your area

A predefined workflow is triggered when you make a request. Although the given workflow may be different, what generally applies is:

- Your request is forwarded to an identity for approval (see Pending requests on page 110/Escalated requests on page 137).
- You are notified whether your request is granted or denied.

Detailed information about this topic

- Requesting products on page 86
- Saved for Later list on page 106
- Managing request templates on page 81
- Pending requests on page 110
- Displaying request history on page 128
- Resubmitting requests on page 128
- Canceling requests on page 129
- Renewing products with limit validity periods on page 130

Setting up and configuring request functions

In order to request products in the Web Portal, the Web Portal must be set up accordingly.

Detailed information about this topic

- Managing request templates

Managing request templates

Request templates help simplify the request process. For example, a request template may contain all the products a new identity needs to get started. If you use a request template to make a request, you are not obliged to request all the products in the template. You only have to select the products you want from it.

Detailed information about this topic

- Requesting using request templates on page 101
- Displaying request templates
- Creating request templates on page 82
- Sharing request templates on page 85
- Editing request templates on page 83
- Deleting request templates on page 85

Displaying request templates

To obtain an overview of all the request templates, you can display them and their associated content. Request templates are sorted by personal and system-wide request templates.

To display request templates

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click **Maintain Templates**.

   This opens the **Cart Templates** page (see Shopping Cart Templates (page description) on page 868).
3. Click **Personal templates** or **System-wide templates** to display the corresponding request templates.

   TIP: Click ▶ (**Expand**) next to the template to expand the contents and display each item.

Related topics

- Requesting using request templates on page 101
- My requests (page description) on page 856
- Shopping Cart Templates (page description) on page 868

Creating request templates

If you request certain products frequently, you can create an request template from an already populated and configured shopping cart that you can reuse later to save time. In addition, you can create a template with products assigned to a different identity.

To create a request template from the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click **Shopping cart**.

   NOTE: The list of products and options for handling them is only shown when there are products in the shopping cart (see Adding products to the shopping cart on page 87).
3. On the **My Shopping Cart** page, click **Actions** > **Create template from shopping cart**.
4. On the **Shopping Cart Templates** page, in the **Name of the new template** field, enter a meaningful name for the request template.
5. Click **Create template**.

To create a request template with another identity's products.

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click the **Start a new request** tile.
3. On the **Request** page, click **Actions** > **Select a reference user**.

4. In the **Select identity** dialog, click the identity in the list whose product requests you want to use as a template.

   A new page lists requests, memberships, and entitlements of the selected identity.
5. On the **Requests for <identity name>** page, click **Create template**.
6. On the **Shopping Cart Templates** page, in the **Name of the new template** field, enter a meaningful name for the request template.
7. Click **Create template**.

Related topics

- Requesting using request templates on page 101
- My requests (page description) on page 856
- My shopping cart (page description) on page 869
- Shopping Cart Templates (page description) on page 868
- Requests for identities (page description) on page 860

Editing request templates

You can edit the details of your request templates. You can also add more products to and remove products from request templates that you created yourself (see Adding products to request templates on page 83 and Removing products from request templates on page 84).

To edit a request template

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click the **Maintain templates** tile.
3. On the **Cart Templates** page, next to the request template that you want to edit, click (**Edit**).
4. In the **Edit template** dialog, in the input fields, enter the desired additional information.

   TIP: You can also share request templates with other users here. For more information, see the Sharing request templates on page 85.
5. Click **Save**.

Detailed information about this topic

- Adding products to request templates on page 83
- Removing products from request templates on page 84

Adding products to request templates

You can add more products to your existing requests templates.

To add a product from the shopping cart to a request template

1. Add the product you want to add to your request template to the shopping cart. For more information, see the Adding products to the shopping cart on page 87.
2. In the menu bar, click **Request** > **My Requests**.
3. On the **My Requests** page, click the **Shopping Cart** tile.
4. On the **My Shopping Cart** page, click **Actions** > **Create template from shopping cart**.
5. On the **Cart Templates** page, next to the request template to which you want to add a product, click **Select**.

To add products of a different identity to a request template

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click the **Start a new request** tile.
3. On the **Request** page, click **Actions** > **Select a reference user**.
4. In the **Select an identity** dialog, in the list, click the identity whose products you want to add to the request template.

   > NOTE: You can extend the identities list to show more information. To do this, click **View settings** > **Additional columns** and select the information you require from the dialog.

   A new page lists requests, memberships, and entitlements of the selected identity.
5. On the **Requests for <identity name>** page, click **Create template**.
6. On the **Cart Templates** page, next to the request template to which you want to add a product, click **Select**.

Related topics

- Requesting products through reference users on page 100
- Requesting using request templates on page 101
- My requests (page description) on page 856
- Request (page description) on page 858
- Requests for identities (page description) on page 860
- My shopping cart (page description) on page 869
- Shopping Cart Templates (page description) on page 868

Removing products from request templates

You can remove products from your request templates.

To remove a product from a request template

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click the **Maintain templates** tile.
3. On the **Cart Templates** page, in front of the template with the product you want to remove, click (**Edit**).
4. Next to the product that you want to remove, click (**Delete**).
5. In the **Change template** dialog, confirm the prompt with **Yes**.

Related topics

- Requesting using request templates on page 101
- My requests (page description) on page 856
- Shopping Cart Templates (page description) on page 868

Sharing request templates

To allow other users to use your request templates, you can share your own request templates with other users.

To share an request template with other users

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click the **Maintain templates** tile.
3. On the **Cart Templates** page, next to the request template that you want to share, click (**Edit**).
4. In the **Edit template** dialog, select the **Template is available to other identities** and **Publication is approved** check boxes.

   NOTE: Enable this option only if you do not want to make any more changes to the request template.
5. Click **Save**.

Related topics

- Requesting using request templates on page 101
- My requests (page description) on page 856
- Shopping Cart Templates (page description) on page 868

Deleting request templates

You can delete request templates at any time.

NOTE: You can only delete your own personal request templates.

To delete a request template

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click the **Maintain templates** tile.
3. On the **Cart Templates** page, next to the request template that you want to delete, click (**Delete**).
4. In the **Delete template** dialog, confirm the prompt with **Yes**.

Related topics

- Requesting using request templates on page 101
- My requests (page description) on page 856
- Shopping Cart Templates (page description) on page 868

Requesting products

A request process is triggered when you request a product. Whether you are authorized to request a product depends on your role and your permissions. Managers or other authorized users can make a request for other identities in their name.

You can complete a request in three steps:

1. Add the desired product to your shopping cart (see Adding products to the shopping cart on page 87).
2. Verify the shopping cart and amend the product requests as required (see Managing products in the shopping cart on page 88).
3. Submit the request (see Submitting requests on page 97).

Detailed information about this topic

- Adding products to the shopping cart on page 87
- Managing products in the shopping cart on page 88
- Submitting requests on page 97
- Requesting products on the Saved for Later list on page 108
- Requesting using request templates on page 101
- Displaying and requesting other identity’s products on page 99
- Requesting for other identities or subidentities on page 98
- Requesting privileged access on page 102
- Requests for Active Directory groups on page 104

Adding products to the shopping cart

To request products, first you must select them and add them to your shopping cart.

To add products to the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. On the **Request** page, perform the following:
   - In the **Find a service item** field, enter the name of the required product and click (**Search in all categories**).
   - Click the tile of service category that contains the product you wan tot request.

   The relevant products are displayed.

   TIP: If you want to change the selected service category, click **Change service category** and then click the service category you require.

   If the service category contains a child category, select the child category you want from the **Service items in the category** menu.

   To display the products of the main categories and subcategories combined, enable the **Include child categories** option.
4. Perform one of the following tasks:
   - Add a product to the shopping cart: Next to the product with the product you want to request, click **Add to cart**.
   - Add multiple products to the shopping cart: Select the appropriate check boxes next to the products you want to request and click **Add to cart** below the list.

   TIP: If you select a product that has dependent products, a dialog opens that allows you to request these products as well.

   NOTE: If you select a product that requires additional information, a corresponding dialog opens.

   NOTE: If you select a group, a dialog opens, where you must enter a name, which gives advice on naming, group type and target container. The approver adds the group based on this information (see Approving pending requests from newly created Active Directory groups on page 114).

   This opens the **Shopping Cart** page. Now, you can check the request and, if necessary, add to each product request (see Managing products in the shopping cart on page 88). Then send the request (see Submitting requests on page 97).

   Or you can continue working in the Web Portal to do things such as add more products.

Related topics

- Managing products in the shopping cart on page 88
- Submitting requests on page 97
- Request (page description) on page 858
- My shopping cart (page description) on page 869

Managing products in the shopping cart

After you have added products to your shopping cart (see Adding products to the shopping cart on page 87), you can delete individual product requests from the cart, add more details to them, or perform other actions.

NOTE: In certain circumstances, you may cause a request to violate compliance rules if it allocates a specific entitlement to a business role. For example, an identity may obtain an unauthorized entitlement through this business role. In this case, the compliance violation is displayed in the details pane of the shopping cart.

To manage products in the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **Shopping Cart** page, edit the shopping cart.
   You can perform the following actions:
   - Remove products from the shopping cart (see Removing products from the shopping cart on page 90)
   - Define the validity of the products (see Setting the validity period of products in your shopping cart on page 91)
   - Change the priority of the requests (see Specifying the priority of products in your shopping cart on page 92)
   - Enter reasons for the requests (see Giving reasons for requests on page 93)
   - Assign a department to products (see Specifying departments for products in shopping cart on page 94)
   - Check the shopping cart for invalid products and remove them (see Checking the shopping cart and removing invalid products on page 95)
   - Request products for multiple identities (see Requesting products in the shopping cart for multiple identities on page 96)
   - Place products on the Saved for Later list (see Saving products for later on page 107
   - Show the Saved for Later list (see Displaying Saved for Later list on page 107)

- Make a template from the shopping cart (see Creating request templates on page 82)

4. Ensure you only have requests that you really want to submit in your cart.

   NOTE: If your shopping cart contains products that you want to request more often, make a template from the shopping cart (see Managing request templates on page 81).

   Now you can send your request (see Submitting requests on page 97).

Related topics

- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- Saved for Later list on page 106
- Managing request templates on page 81
- Request (page description) on page 858
- My shopping cart (page description) on page 869

Displaying the shopping cart

After you have added products to your shopping cart (see Adding products to the shopping cart on page 87), you can view all the products in your shopping cart along with their details.

To display the products in your shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.

   This opens the **My Shopping Cart** page (see My shopping cart (page description) on page 869).
3. Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

Related topics

- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Editing multiple products in the shopping cart

After you have added products to the shopping cart (see Adding products to the shopping cart on page 87), you can modify further settings for single or all products in the shopping cart (see Setting the validity period of products in your shopping cart on page 91, Specifying the priority of products in your shopping cart on page 92, Giving reasons for requests on page 93, Specifying departments for products in shopping cart on page 94). If you have several products in the shopping cart, you can edit them in the overview and apply the modified properties to multiple products. This way, you do not have to adjust the same settings separately for each individual product, but can "copy" the changes.

To editing multiple products in the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, click **Actions** > **Edit details**.
4. On the **Details** page, expand the product details that you want to edit.

   If a product is in the shopping cart more than once, the individual items are displayed one below the other.
5. Change the settings as required.

   > TIP: If you want to change the properties for all the same products in the shopping cart, click **Apply to all**.
6. Click **Save**.

   Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

Related topics

- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- Requesting products on page 86
- My requests (page description) on page 856
- Details (page description) on page 873

Removing products from the shopping cart

After adding added products to your shopping cart (see Adding products to the shopping cart on page 87), you can remove them again.

To remove products from the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, in the list, click the product that you do not want to request anymore.
4. In the details pane, click **Delete**.
5. In the dialog, confirm the prompt with **Yes**.

   Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

To remove all products from the shopping cart

- Delete the shopping cart. For more information, see Deleting shopping carts on page 97.

Related topics

- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Setting the validity period of products in your shopping cart

After you have added products to your shopping cart (see Adding products to the shopping cart on page 87), you can set their validity period. Once a product's validity period has expired, it can no longer be used.

NOTE: If you alter the validity period, the request's validity is determined by this information and not from the date of approval. An additional message is shown in the details pane of the respective product. If the request approval validity period has expired, the request is annulled.

TIP: You can renew the validity of a currently assigned product. For more information, see Renewing products with limit validity periods on page 130.

To set the validity period of a product in the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, click the product in the list whose validity you want to define.
4. In the details pane, in the **Valid from** field, specify from when the product is valid.

5. In the **Valid until** field, specify until when the product is valid.
6. Click **Save**.

   Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

To set the validity period of all products in the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, click **Edit**.
4. In the dialog, check the **Valid from** box.
5. In the **Valid from** field, specify from when the products are valid.

   NOTE: Products that already have a fixed validity period are not changed in the process. To change the validity period of products that already have a fixed validity period, check the **Replace already specified dates** box.
6. In the **Valid until** field, specify until when the products are valid.

   NOTE: Products that already have a fixed validity period are not changed in the process. To change the validity period of products that already have a fixed validity period, check the **Replace already specified dates** box.
7. Click **Save**.

   Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

Related topics

- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Specifying the priority of products in your shopping cart

After you have added products to your shopping cart (see Adding products to the shopping cart on page 87), you can specify their priority. The priority allows approvers to quickly identify how important a product request is.

To specify the priority of a product in the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.

3. On the **My Shopping Cart** page, click the product in the list whose priority you want to define.
4. In the details pane, in the **Priority** menu, select the priority.
5. Click **Save**.

   Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

To specify the priority of all products in the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, click **Edit**.
4. In the dialog, select the check box next to **Apply the following priority to all products in the shopping cart**.
5. In the menu, select the desired priority.
6. Click **Save**.

   Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

Related topics

- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Giving reasons for requests

After you have added products to your shopping cart (see Adding products to the shopping cart on page 87), you can give reasons for requesting them. A reason can help approvers make their approval decisions.

To give a reason for requesting a product from the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, click the product in the list whose request you want to justify.
4. In the details pane, in the **Reason** field, enter your reason for requesting this product.
5. Click **Save**.

Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

To give a reason for requesting all products from the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, click **Edit**.
4. In the details pane, in the **Reason** field, enter your reason for requesting these products.
5. Click **Save**.

   Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

Related topics

- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Specifying departments for products in shopping cart

After you have added products to the shopping cart (see Adding products to the shopping cart on page 87), you can assign products to departments. This assignment can be used for billing purposes, for example.

To assign a department to a product in the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, in the list, click the product to which you want to assign a department.
4. In the details pane, next to the **Department** field, click **Assign**.

   TIP: If the product already has an department, click **Change**.
5. In the **Department** dialog, click the department you want to assign to the product.
6. On the **My Shopping Cart** page, click **Save** in the details pane.

   Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

Related topics

- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Checking the shopping cart and removing invalid products

When you send a request, it is automatically checked to see if it contains invalid products. You can also run this check before you submit the request. If necessary, you will be shown why specific product requests are invalid. You can then remove any invalid products from the shopping cart.

To check your shopping cart for invalid products

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, perform one of the following actions:
    - Click **Actions** > **Check shopping cart**.
    - Click **Submit**.

      NOTE: If the check is successful, the request can be submitted.

   If invalid products are found, the **Request cannot be submitted** dialog opens.
4. (Optional) In the **Request cannot be submitted** dialog, click **OK**.

   On the **My Shopping Cart** page, in the **Status** column, symbols and information are shown about the invalid products.

   Table 21: Checking status

Icon	Status
	Request can be made.
	Request violates a rule but can still be made. This icon can also indicate that a mandatory product is missing.
	Request cannot be made due to missing request permissions. Or the product has already been assigned.
Advice	If the request verification is still pending, a message is shown in the details pane.

5. In the list, click the invalid product.

In the details pane, the relevant message is displayed that gives you precise information about why you cannot request the product.

To remove all invalid products from the shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click the **Shopping cart** tile.
3. On the **My Shopping Cart** page, perform one of the following actions:
   - Click **Submit**.

     NOTE: If the check is successful, the request can be submitted.
   - Click **Actions** > **Check shopping cart**.

   If invalid products are found, the **Request cannot be submitted** dialog opens.
4. In the **Request cannot be submitted** dialog, click **OK**.
5. Click **Actions** > **Delete invalid requests**.
6. In the **Delete invalid requests** dialog, confirm the prompt with **Yes**.

Related topics

- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Requesting products in the shopping cart for multiple identities

After you have added products to your shopping cart (see Adding products to the shopping cart on page 87), you can request the products in your shopping cart for other identities as well.

To request a product in the shopping cart for multiple identities

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, in the list, click the product that you want to request for other identities.
4. In the details pane, click **Actions** > **Request for multiple identities**.
5. In the **Request for multiple identities** dialog, click the identity you want to request the product for.
6. Click **Save**.

Now you can add more products to your shopping cart, set additional options for products in the shopping cart, or submit the request.

Related topics

- Requesting for other identities or subidentities on page 98
- Adding products to the shopping cart on page 87
- Submitting requests on page 97
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Deleting shopping carts

You can clear your shopping cart at any time.

To delete your shopping cart

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, click **Actions** > **Delete shopping cart**.
4. In the dialog, confirm the prompt with **Yes**.

Related topics

- Removing products from the shopping cart on page 90
- Adding products to the shopping cart on page 87
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Submitting requests

After you have added products to your shopping cart (see Adding products to the shopping cart on page 87), and edited and, if necessary, checked the request (see Managing products in the shopping cart on page 88), you can submit your shopping cart.

To submit your requests

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping CartShopping Cart** page, click .

   This checks, submits, and triggers the request workflow.

TIP: To check the request's validity before you submit the request, click **Actions** > **Check shopping cart**. You can solve most problems of invalid product requests in the shopping cart by removing the problem product from the shopping cart (see Checking the shopping cart and removing invalid products on page 95 and Removing products from the shopping cart on page 90).

NOTE: You may be required to confirm the terms of use for some shopping cart items. The terms of use are displayed after you have confirmed the prompt with **Yes**. Read the terms of use and set the option **I have read and understood the terms of use**. You will also be prompted to enter your user name and password. Close the terms of use view and click **Accept**. For more information about the terms of use, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- Adding products to the shopping cart on page 87
- Managing products in the shopping cart on page 88
- Checking the shopping cart and removing invalid products on page 95
- Removing products from the shopping cart on page 90
- My requests (page description) on page 856
- Request (page description) on page 858
- My shopping cart (page description) on page 869

Requesting for other identities or subidentities

You can make requests for other identities (such as department managers). You can only request products from the shops where the identity is a customer and for which you are responsible.

If you are logged in to the Web Portal with your main identity, you can trigger a request for yourself and for your subidentities at the same time. If you are logged in with your subidentity, you can only make requests for the current subidentity.

TIP: You can also request products for other identities directly from the shopping cart. For more information, see Requesting products in the shopping cart for multiple identities on page 96.

To request products for another identity

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. On the **Request** page, click **Change** next to the **Recipient** field.

4. In the **Recipients** dialog, in the list, click the identity who is going to receive the products.

   NOTE: You can extend the identities list to show more information. To do this, click **View settings** > **Additional columns** and select the information you require from the dialog.

   The selected identities are listed under **Selected**.

   TIP: To remove an identity from the recipient list, click the respective identity under **Selected**.

5. Click **Close**.
6. Add the products that you want to request for the selected identity to the shopping cart (see Adding products to the shopping cart on page 87).

   TIP: If you want to find out which products are already assigned to the selected recipients, on the **Request** page, click **Actions** > **Check requests for this recipient**.

7. (Optional) Edit the shopping cart (see Managing products in the shopping cart on page 88).
8. Submit the request (see Submitting requests on page 97).

Related topics

- Requesting products in the shopping cart for multiple identities on page 96
- My requests (page description) on page 856
- Request (page description) on page 858

Displaying and requesting other identity’s products

You can request products that other identities already own. The Web Portal offers you various options for this:

- Request by reference user: You can display all the products of a specific identity and request them as well.
- Request by peer groups: You can display and request products that other identities within your system have already requested. As a manager, you can also see products from the peer group of an identity that you manage.

Related topics

- Requesting products in the shopping cart for multiple identities on page 96
- Requesting for other identities or subidentities on page 98

Requesting products through reference users

You can request products that a particular identity already owns. This is called requesting by reference user.

Products you cannot request are marked with a red cross in the product view.

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. On the **Request**/ page, click **Actions** > **Select a reference user**.
4. In the **Select an identity** dialog, in the list, click the identity whose products you also want to request.

   NOTE: You can extend the identities list to show more information. To do this, click **View settings** > **Additional columns** and select the information you require from the dialog.

   This opens the **Requests for <identity>** page and lists requests, memberships, and entitlements of the selected identity (see Requests for identities (page description) on page 860).
5. Add the products that you want to save for later, to the shopping cart (see Adding products to the shopping cart on page 87).
6. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

Related topics

- Requesting products through peer groups on page 100
- Managing products in the shopping cart on page 88
- Requesting using request templates on page 101
- My requests (page description) on page 856
- Request (page description) on page 858
- My shopping cart (page description) on page 869

Requesting products through peer groups

You can see and request products that other identities within your environment have already requested. As a manager, you can also see products from the peer group of an identity that you manage. This way, you have a quick method of requesting products that are important to you or your responsible identities.

A peer group contains all the identities that have the same manager or the same primary or secondary department as the request recipient.

To request other identities' products

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. (Optional) If you want to make a request for another identity or check which products have been requested by their peer group, proceeds as follows:
    a. On the **Request** page, click **Change** next to the **Recipient** field.
    b. In the **Recipients** dialog, in the list, click the identity who is going to receive the products.

       NOTE: The list may contain a maximum of one identity. To remove an identity from the list, click on the respective identity.

    c. Click **Close**.
4. On the **Request** page, click **Actions** > **Show products other identities requested**.

   This opens the **Products other identities requested** page that lists requests, memberships, and the peer groups of the selected identity (see Products other identities requested (page description) on page 861).
5. Add the products that you want to save for later, to the shopping cart (see Adding products to the shopping cart on page 87).
6. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

Related topics

- Requesting products through reference users on page 100
- Managing products in the shopping cart on page 88
- Requesting using request templates on page 101
- My requests (page description) on page 856
- Request (page description) on page 858
- Products other identities requested (page description) on page 861
- My shopping cart (page description) on page 869

Requesting using request templates

You can use your own (private) request templates or request templates that are shared with all users (public) for making requests. This helps simplify proper provisioning for a particular job or function. For example, a template may contain all the products a new identity needs to get started. If you use a template for a request, you are not obliged to request all the products in the template. You only have to select the products you want from the template.

TIP: To find out how you can request the same products as another identity, see Requesting products through reference users on page 100.

To request products using a request template

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. On the **Request** page, click **Actions** > **Select a request template**.
4. In the **Choose a template** dialog, next to the required request template, click **Add to cart**.

   TIP: If you want to display all of the content of the request templates, click ▶ next to the request template.
5. On the **My Shopping CartShopping Cart** page, click .

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

Related topics

- Managing request templates
- Meine Bestellvorlagen verwalten
- Managing products in the shopping cart on page 88
- Requesting products through reference users on page 100
- Shopping Cart Templates (page description) on page 868
- My requests (page description) on page 856
- Request (page description) on page 858
- My shopping cart (page description) on page 869

Requesting privileged access

You can use the **Privileged access requests** service category to request privileged access to high-security systems (Privileged Account Management systems).

TIP: For more information on the topic of Privileged Account Management, see the *One Identity Manager Administration Guide for Privileged Account Governance*.

To request privileged access

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Start a new request**.

3. On the **Request** page, click **Privileged access requests**.
4. On the **Request** page, select how you want to access the system by selecting the check box in front of the corresponding option:
   - **Password release request**: Request a temporary password.
   - **Remote desktop session request**: Request temporary access through a remote desktop connection.
   - **SSH key request**: Request temporarily valid SSH key.
   - **SSH session request**: Request temporary access through an SSH session.
   - **Telnet session requests**: Request temporary access using a Telnet session.
5. Click **Add to cart**.
6. In the new dialog, next to **PAM user account**, click **Assign/Change**.
7. In the **PAM user account** dialog, select the PAM user account that you want to use for PAM access.
8. Depending on the type of access you have selected, perform one of the following actions:
   - Password request:
     1. Next to **System to access**, click **Assign**.
     2. In the **System to access** dialog, select whether you want to request access for a **PAM asset** or a **PAM directory**.
     3. Click the corresponding PAM directory or PAM asset.
   - Telnet session request, remote desktop session request, SSH key request, or SSH session request:
     1. Next to **Asset**, click **Assign**.
     2. In the **Asset** dialog, click the corresponding PAM asset.
9. Perform the following actions:
   a. Next to **Account to access**, click **Assign**.
   b. In the **Account to access** dialog, select which access you want to request, either **PAM directory account** or a **PAM Asset account**.
   c. Click the PAM asset account or PAM directory account you want to access.
10. (Optional) In the **Comment** field, enter a comment, for example, to justify why you are requesting this access.
11. In the **Valid from** field, specify the time from which you want the access to be valid or clear the check box so that access is valid from the time of this request.

    TIP: Use the icons next to the date field to select the date and time from the calendar or a list.
12. In **Checkout duration**, enter the number of minutes for which the access is valid.

NOTE: This duration refers to your entry in the **Valid from** field. For example, if you have specified that the access is valid from 12 noon tomorrow and should be valid for 60 minutes, then the validity period will expire at 1 pm tomorrow.

13. Click **Save**.
14. (Optional) Repeat the steps for all other users and access types.
15. On the **My Shopping CartShopping Cart** page, click .

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    Once the request has been approved, a button will appear in the request details pane of the request history (see Displaying request history on page 128) that you can use to log in to the Privileged Account Management system to obtain the login credentials.

Related topics

- Managing products in the shopping cart on page 88
- My requests (page description) on page 856
- Request (page description) on page 858
- My shopping cart (page description) on page 869

Requests for Active Directory groups

To manage Active Directory groups, you can make different requests.

Detailed information about this topic

- Requesting new Active Directory groups on page 104
- Displaying and editing my system entitlements main data on page 409
- Displaying and editing system entitlements main data on page 743
- Deleting my Active Directory groups on page 410
- Deleting Active Directory groups on page 744

Requesting new Active Directory groups

To create a new Active Directory group, you must request either the **Create an Active Directory security group** product or the **Create an Active Directory distribution group** product.

To request a new Active Directory group

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. Click the service category **Active Directory groups** on the **Request** page.
4. Select the check box in front of **New Active Directory security group** or the **New Active Directory distribution group** product.
5. Click **Add to cart**.
6. In the dialog, enter a name for the new group in the **Group** name input field.
7. Click **OK**.

   TIP: Enter a group name that details the naming, type of group and target container. The approver adds the group based on this information.
8. On the **My Shopping Cart** page, click on the request you just added in the list.
9. In the details pane, perform one of the following actions:
   - As a requester without responsibility for the target system, check the name for the new group in the **Suggested name** field.
   - As the target system manager, provide additional details about the new group:
     - **Name**: Enter a name for the group.
     - **Group scope**: Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can select one of the following group scopes:
       - **Global group**: Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group’s domain.
       - **Local**: Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.
       - **Universal**: Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
     - **Container**: Click **Assign** and select a container for the group.
10. In the details pane, click **Save**.
11. Click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

Related topics

- Approving pending requests from newly created Active Directory groups on page 114
- My requests (page description) on page 856
- Request (page description) on page 858
- My shopping cart (page description) on page 869

Requesting new SharePoint groups

To create a new SharePoint group, you must request the **New SharePoint Group** product.

To request a new SharePoint group

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. Click the service category **SharePoint groups** on the **Request** page.
4. Select the check box next to **New SharePoint group**.
5. Click **Add to cart**.
6. In the dialog, enter a name for the new group in the **Group** name input field.

   TIP: Enter a group name that details the naming, type of group and target container. The approver adds the group based on this information.
7. Click **OK**.
8. Click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

Related topics

- Approving pending requests from newly created SharePoint groups on page 116
- My requests (page description) on page 856
- Request (page description) on page 858
- My shopping cart (page description) on page 869

Saved for Later list

In your Saved for Later list you can save products that you want to request at a later date. For more information about the **Saved for Later** page, see Saved for Later list (page description) on page 871.

Detailed information about this topic

- Saving products for later on page 107
- Displaying Saved for Later list on page 107
- Requesting products on the Saved for Later list on page 108
- Removing products from the Saved for Later list on page 109
- Deleting the Saved for Later list on page 110

Saving products for later

If you do not want to request products immediately but at a later date, you can save the products on the Saved for Later list. You can access your Saved for Later list at any time, move products from it into your shopping cart, and request them (see Requesting products on the Saved for Later list on page 108).

To add a product to your Saved for Later list.

1. Add the product that you want to save for later, to the shopping cart (see Adding products to the shopping cart on page 87).
2. In the menu bar, click **Request** > **My Requests**.
3. On the **My requests** page, click **Shopping cart**.
4. On the **My Shopping Cart** page, click the product in the list that you want to save for later.
5. In the details pane, click (**Actions**) > **Save for later**.

   The product is moved with all its settings to your shopping cart.

Related topics

- Managing products in the shopping cart on page 88
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Displaying Saved for Later list

After you have moved products to your Saved for Later list, you can display all the products saved there.

To display your Saved for Later list

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, perform one of the following actions:
   - If there are products in the shopping cart, click **Actions** > **View Saved for Later**.
   - If the shopping cart is empty, click **Saved for later**.

   This opens the **Saved For Later** page (see Saved for Later list (page description) on page 871).

Related topics

- Managing products in the shopping cart on page 88
- My requests (page description) on page 856
- My shopping cart (page description) on page 869

Requesting products on the Saved for Later list

To request products on your Saved for Later list, you must add the products to your shopping cart.

To move products from the Saved for Later list to the shopping cart and request them

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, perform one of the following actions:
   - If there are products in the shopping cart, click **Actions** > **View Saved for Later**.
   - If the shopping cart is empty, click **Saved for later**.
4. On the **Saved for Later** page, select the check boxes in front of the products in the list that you want to request or add to the shopping cart.
5. Click **Move to shopping cart**.

   This moves the products and all their settings to your shopping cart.
6. On the **My Shopping CartShopping Cart** page, click .

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

Related topics

- Managing products in the shopping cart on page 88
- Submitting requests on page 97
- My requests (page description) on page 856
- My shopping cart (page description) on page 869
- Saved for Later list (page description) on page 871

Removing products from the Saved for Later list

You can remove products from your Saved for Later list. To delete the entire Saved for Later list, see Deleting the Saved for Later list on page 110.

To remove a product from your Saved for Later list

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, perform one of the following actions:
    - If there are products in the shopping cart, click **Actions** > **View Saved for Later**.
    - If the shopping cart is empty, click **Saved for later**.
4. On the **Saved for Later** page, in the list, click the product that you want to remove from the Save for Later list.
5. In the details pane, click (**Delete this request.**).
6. Confirm the prompt with **Yes** in the dialog.

To remove multiple products from your Saved for Later list

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My Requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, perform one of the following actions:
    - If there are products in the shopping cart, click **Actions** > **View Saved for Later**.
    - If the shopping cart is empty, click **Saved for later**.
4. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you want to remove from the Save for Later list.
5. Click **Delete selected**.
6. In the **Saved for Later** dialog, confirm the prompt with **Yes**.

Related topics

- Managing products in the shopping cart on page 88
- My requests (page description) on page 856
- My shopping cart (page description) on page 869
- Saved for Later list (page description) on page 871

Deleting the Saved for Later list

You can delete your Saved for Later list. For more information about removing individual products, see Removing products from the Saved for Later list on page 109.

To delete your Saved for Later list

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Shopping cart**.
3. On the **My Shopping Cart** page, perform one of the following actions:
    - If there are products in the shopping cart, click **Actions** > **View Saved for Later**.
    - If the shopping cart is empty, click **Saved for later**.
4. On the **Saved for Later** page, click **Delete Saved for Later list**.
5. In the **Saved for Later** dialog, confirm the prompt with **Yes**.

Related topics

- Managing products in the shopping cart on page 88
- My requests (page description) on page 856
- My shopping cart (page description) on page 869
- Saved for Later list (page description) on page 871

Pending requests

Many requests go through a manual approval process in order to ensure the correct assignment of products. If the request requires approving or denying, the request classifies as pending and as approver you can make the approval decision. If you need more information to make an approval decision, you can submit an inquiry, add more approvers, or reroute the request. For more information about the **Pending requests** page, see Pending attestations (page description) on page 875.

Detailed information about this topic

- Displaying pending requests on page 111
- Approving and denying requests on page 111
- Appointing other approvers for pending requests on page 118
- Rejecting request approval on page 122
- Changing priority of pending requests on page 123
- Confirming terms of use on page 124
- Adding more products to pending requests on page 124
- Canceling pending requests on page 125
- Sending inquiries about pending requests on page 125
- Revoking hold status of pending requests on page 127

Displaying pending requests

If you are the approver of certain products and identities request these products, you can display the requests. Then you can make approval decisions about the pending requests (see Approving and denying requests on page 111).

To display pending requests

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.

   This opens the **Pending Requests** page (see Pending attestations (page description) on page 875).
3. (Optional) To display details of a pending request, click the request whose details you want to see.

Related topics

- Displaying escalated requests on page 137
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Approving and denying requests

If you are the approver of a particular product and an identity makes a request for this product, you can grant or deny approval for the request. If you approve a request, the product is available to the identity.

To make an approval decision about a pending request

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, perform one of the following actions:
   - To approve a request, click (**Approve**) next to the request.
   - To deny a request, click (**Deny**) next to the request.

   TIP: To grant or deny approval for all the requests displayed, click (**Approve all**) or (**Deny all**).
4. Click **Next**.
5. (Optional) On the **Pending Requests – Approvals** page, perform the following actions:
   - For approved requests:
     - To provide a reason for all approved requests, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all approved requests, select the reason in the **Standard reason** list.
   - For denied requests:
     - To provide a reason for all denied requests, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all denied requests, select the reason in the **Standard reason** list.
   - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

   TIP: By giving reasons, your approvals are more transparent and support the audit trail.

   NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
6. (Optional) To specify the validity period for a requested product, perform the following actions:
   a. In the list, in the **Valid from** column, click on a value.
   b. In the **Valid from** dialog, specify from when the product is valid.
   c. Click **Close**.
   d. In the list, in the **Valid until** column, click on a value.
   e. In the **Valid until** dialog, specify until when the product is valid.
7. Click **Save**.

Related topics

- Approving and denying escalated requests on page 138
- Displaying and approving entire requests of pending requests on page 113
- Approving pending requests from newly created Active Directory groups on page 114
- Approving new managers' pending requests on page 117
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Displaying and approving entire requests of pending requests

You can see all other products of a product request that are included in this request (meaning, they were sent in the same shopping cart). You can approve pending requests together.

To display an entire request and approve all the requests contained in it.

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, mark the product in the list that has the request you want to see in its entirety.
4. In the details pane, click **more** > **Show entire request**.
5. On the **Request overview** page, click **Approve all**.
6. On the **Pending Requests - Approvals** page, perform one of the following actions:
    - To provide a reason for all request approvals, enter the reason in the **Reason for approvals** field.
    - To use a predefined standard reason for all request approvals, select the reason in the **Standard reason**.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
7. (Optional) To specify the validity period for a requested product, perform the following actions:
    a. In the list, in the **Valid from** column, click on a value.
    b. In the **Valid from** dialog, specify from when the product is valid.

c. Click **Close**.

d. In the list, in the **Valid until** column, click on a value.

e. In the **Valid until** dialog, specify until when the product is valid.

8. Click **Save**.

Related topics

- Displaying and approving entire requests of escalated requests on page 140
- My actions (page description) on page 873
- Pending attestations (page description) on page 875
- Requests overview (page description) on page 878
- Pending requests – Approvals on page 880

Approving pending requests from newly created Active Directory groups

Identities can create Active Directory groups by requesting the **New Active Directory security group** or the **New Active Directory distribution group** product. As approver, you can make approval decisions about requests like this. If you approve the request, you must provide additional information about the group.

To approve a request to create a new Active Directory group

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, click the request for the new Active Directory group in the list.
4. In the details pane, click **Configure the new group**.
5. In the dialog, enter additional information about the new group:
    - **Name**: Enter a name for the group.
    - **Group scope**: Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can select one of the following group scopes:
        - **Global group**: Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group’s domain.
        - **Local**: Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.

        - **Universal**: Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
    - **Container**: Click **Assign**/**Change** and select a container for the group.
6. Click **OK**.
7. Next to the request, click ☑ (**Approve**).
8. Click **Next**.
9. On the **Pending Requests - Approvals** page, perform one of the following actions:
    - To provide a reason for all request approvals, enter the reason in the **Reason for approvals** field.
    - To use a predefined standard reason for all request approvals, select the reason in the **Standard reason**.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. (Optional) To specify the validity period for a requested product, perform the following actions:
    a. In the list, in the **Valid from** column, click on a value.
    b. In the **Valid from** dialog, specify from when the product is valid.
    c. Click **Close**.
    d. In the list, in the **Valid until** column, click on a value.
    e. In the **Valid until** dialog, specify until when the product is valid.
11. Click **Save**.

Related topics

- Requesting new Active Directory groups on page 104
- Approving escalated requests from newly created Active Directory groups on page 141
- My actions (page description) on page 873
- Pending requests on page 110
- Pending requests – Approvals on page 880

Approving pending requests from newly created SharePoint groups

Identities can create SharePoint groups by requesting the **New SharePoint group** product. As approver, you can make approval decisions about requests like this. If you approve the request, you must provide additional information about the group.

To approve a request to create a new SharePoint group

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, click the request for the new SharePoint group in the list.
4. In the details pane, click **Enter information for the new group**.
5. In the dialog, enter additional information about the new group:
    - **Site collection**: Select a site collection where the group will be applied. A site collection groups sites together. User account and their access permissions are managed on the sites.
    - **Display name**: Enter a name for the new group.
    - **Description**: Enter a description for the SharePoint group.
6. Click **OK**.
7. Next to the request, click ☑ (**Approve**).
8. Click **Next**.
9. On the **Pending Requests - Approvals** page, perform one of the following actions:
    - To provide a reason for all request approvals, enter the reason in the **Reason for approvals** field.
    - To use a predefined standard reason for all request approvals, select the reason in the **Standard reason**.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. (Optional) To specify the validity period for a requested product, perform the following actions:
    a. In the list, in the **Valid from** column, click on a value.
    b. In the **Valid from** dialog, specify from when the product is valid.
    c. Click **Close**.

d. In the list, in the **Valid until** column, click on a value.
e. In the **Valid until** dialog, specify until when the product is valid.

11. Click **Save**.

Related topics

- Requesting new SharePoint groups on page 106
- Approving escalated requests from newly created SharePoint groups on page 142
- My actions (page description) on page 873
- Pending requests on page 110
- Pending requests – Approvals on page 880

Approving new managers' pending requests

Managers can allocate new managers for their identities. To do this, they must select the new manager and a deadline in the future for changing managers (see Assigning other managers to my identities on page 299). An assignment of this type triggers a request of type **New manager assignment**.

If you have been selected as the new manger by the manager change, you receive an approval request from the previous manager. After you have accepted the change of manager, you automatically become the new manager on the given date.

You can cancel entitlements already assigned to the identity on the given date.

To approve an escalated assignment to a new manager

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, click the **New manager assignment** request in the list.
4. In the details pane, click **Show the identity's entitlements**.
5. (Optional) If the identity has already been assigned entitlements or products, these will be removed or unsubscribed by default on the effective date. If you want the identity to retain these entitlements or products when transferring to the new manager, in the **New manager assignment** dialog, disable the check boxes next to the respective entitlements and products.
6. Click **Save**.
7. Next to the request, click (**Approve**).
8. Click **Next**.
9. On the **Pending Requests - Approvals** page, perform one of the following actions:

- To provide a reason for all request approvals, enter the reason in the **Reason for approvals** field.
- To use a predefined standard reason for all request approvals, select the reason in the **Standard reason**.
- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

10. (Optional) To specify from when the new manager is responsible for the identity, perform the following:
    a. Click **Valid from**.
    b. In the **Valid from** field in the dialog, enter the date from which you want the new manager to take over.
    c. Click **Close**.
11. Click **Save**.

Related topics

- Assigning other managers to my identities on page 299
- Approving new manager's escalated assignments on page 144
- My actions (page description) on page 873
- Pending attestations (page description) on page 875
- Pending requests – Approvals on page 880

Appointing other approvers for pending requests

You can give an another identity the task of approving a product request. To do this, you have the following options:

- Reroute approval
  You give the task of approving to another approval level (see Rerouting approvals of pending requests on page 119).
- Appoint additional approver
  You can give an another identity the task of approving (see Appointing additional approvers to pending requests on page 120). The additional approver must make an approval decision in addition to the other approvers.
  The additional approver can reject the approval and return it to you (see Rejecting

request approval on page 122).
You can withdraw an additional approver. For example, if the other approver is not available.

- Delegate approval
  You delegate the task of approving to another approval level (see Delegating approvals of pending requests to other identities on page 121). This identity is added as approver in the current approval step and makes approval decisions on your behalf.
  The new approver can reject the approval and return it to you (see Rejecting request approval on page 122).
  You can withdraw a delegation and delegate another identity. For example, if the other approver is not available.
- Escalate approval

  You escalate the approval (see Escalating approvals of pending requests on page 122). The request is presented to another approval body. The request is then further processed in the normal approval workflow.

Rerouting approvals of pending requests

You can let another approval level of the approval workflow make the approval decision about a product. For example, if approval is required by a manager in a one-off case.

To reroute an approval

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, in the list, click the request with the approval that you want to reroute.
4. In the details pane, click **more** > **Reroute approval**.
5. In the **Reroute approval** dialog next to the approval level that you want to reroute to, click **Reroute approval**.
6. (Optional) In the dialog, enter a reason for rerouting.
7. Click **Reroute approval**.

Related topics

- Rerouting escalated requests' approvals on page 145
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Appointing additional approvers to pending requests

You can give another identity the task of approving a product request. The additional approver must make an approval decision in addition to the other approvers.

To add an additional approver

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, click the request in the list to which you want to add an additional approver.
4. In the details pane, click **more** > **Add approver**.
5. In the **Select additional approver** dialog, click the identity you want to act as an additional approver.
6. In the dialog, enter a reason for adding the additional approver.
7. Click **Save**.

Related topics

- Removing additional approvers of pending requests on page 120
- Appointing additional approvers to escalated requests on page 146
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Removing additional approvers of pending requests

If you have given the task of approving a product request to another identity, you can remove this additional approver as long as the product has the status **Request**. Once the additional approver has been removed, the original approvers are the only approvers for this request and you can add a new additional approver.

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, in the list, click the request to which you added an additional approver.
4. In the details pane, click **Withdraw additional approval**.
5. In the dialog, enter a reason for withdrawing the approver.
6. Click **Save**.

Related topics

- Appointing additional approvers to pending requests on page 120
- Removing additional approvers from escalated requests on page 147
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Delegating approvals of pending requests to other identities

You can delegate an approval decision about a request to another identity. You can revoke this action in the approval history (see Withdrawing delegations from pending requests on page 121).

To delegate an approval

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, in the list, click the request whose approval decision you want to delegate to another identity.
4. In the details pane, click **more** > **Delegate approval**.
5. In the **Select an identity that is allowed to approve** dialog, click the identity to which you want delegate the approval.
6. In the dialog, enter a reason for the delegation.
7. Click **Save**.

Related topics

- Withdrawing delegations from pending requests on page 121
- Delegating approvals of escalated requests to other identities on page 147
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Withdrawing delegations from pending requests

If a request's approval has been delegated to another identity, you can withdraw the delegation.

To withdraw an approval delegation

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Approval History**.

3. On the **Approval History** page, in the list, click the request with the approval delegation you want to withdraw.
4. In the details pane, click **Withdraw delegation**.
5. In the dialog, enter a reason why you are withdrawing the approval delegation.
6. Click **Save**.

Related topics

- Delegating approvals of pending requests to other identities on page 121
- Withdrawing delegations from escalated requests on page 148
- My actions (page description) on page 873
- Approval history (page description) on page 881

Escalating approvals of pending requests

You can escalate the approval of a product request. The request is presented to another approval body. The request is then further processed in the normal approval workflow.

To escalate approval for a request

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, click the request in the list whose approval you want to escalate.
4. In the details pane, click **more** > **Escalate approval**.
5. In the dialog, enter a reason for the escalation.
6. Click **Save**.

Related topics

- Escalated requests on page 137
- Escalated requests on page 137
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Rejecting request approval

If you have been added to a product request as an additional approver or the approval of the product request was passed to you, you can reject the approval and return the request to the original approver.

To reject an approval

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, in the list, click the request that do not want to make an approval decision about.
4. In the details pane, click **more** > **Reject approval**.
5. In the dialog, enter a reason for the rejecting.
6. Click **Save**.

Related topics

- Appointing additional approvers to pending requests on page 120
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Changing priority of pending requests

As an approver of requests, you can set the priority of individual requests. For example, this positions requests at different positions in the request list. This means that if the list is sorted in descending order, requests with high priority are listed at the top.

To change a request's priority

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, click the request in the list whose priority you want to change.
4. In the details pane, click **more** > **Change priority**.
5. In the **Set the priority for this request** dialog, in the **Priority** menu, click the priority you want to use for this request.
6. Click **Apply**.
7. Then make an approval decision about the request (see Approving and denying requests on page 111).

   NOTE: The modified priority is not changed until you have saved you approval decision about the request.

Related topics

- Approving and denying requests on page 111
- Changing priority of escalated requests on page 148

- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Confirming terms of use

If a product has been requested for you by another identity that requires confirmation of the terms of use, your approval is required for that request.

To confirm terms of use of a request if you are the recipient

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, click the request in the list that requires confirmation of the terms of use.
4. In the details pane, click **Show details**.
5. Read the terms of use carefully and select the **I have read and understood the terms of use** check box.
6. Click **Accept**.

Related topics

- My actions (page description) on page 873
- Pending attestations (page description) on page 875
- Pending requests – Approvals on page 880

Adding more products to pending requests

You can add more products to requests.

To add more products to a request

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Requests** page, click the request in the list that you want to add products to.
4. In the details pane, click **more** > **Show entire request**.
5. On the **Request overview** page, click **Add items to this request**.
6. On the **Request** page, add the product you want to the shopping cart, edit the products in the shopping cart and send the request.

Related topics

- Adding products to the shopping cart on page 87
- Managing products in the shopping cart on page 88
- Submitting requests on page 97
- Displaying and approving entire requests of pending requests on page 113
- Adding more products to escalated requests on page 149
- My actions (page description) on page 873
- Pending attestations (page description) on page 875
- Requests overview (page description) on page 878
- Request (page description) on page 858

Canceling pending requests

As approver, you can cancel a request. This cancels the request and the requested product is not assigned to the recipient but it can be requested again.

> TIP: To find out how to cancel requests for yourself or for identities that you manage, see Canceling requests on page 129.

To cancel a pending request

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending requests** page, mark the request in the list that you want to cancel.
4. In the details pane, click **Withdraw request**.
5. In the **Withdraw request** dialog, enter a reason for the cancellation.
6. Click **OK**.

Related topics

- Canceling requests on page 129
- Canceling escalated requests on page 150
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Sending inquiries about pending requests

Before you make an approval decision about a request, you can send a question to an identity about it.

NOTE: Once an inquiry has been made about a request, it is given hold status in the approval workflow. Only the originator of the inquiry (or the chief approval team) can make an approval decision about a request with hold status. You can revoke hold status with the following actions:

- Delete the inquiry (see Deleting inquiries about pending requests on page 126)
- Revoke the status after answering the question (see Revoking hold status of pending requests on page 127)

To make an inquiry

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Attestations** page, in the list, click the request that you want to inquire about.
4. In the details pane, click **more** > **Send inquiry**.
5. In the **Submit an inquiry about this request** dialog, click the identity to which you want send the inquiry.
6. In the **Submit an inquiry about this request** dialog, enter your question in the **Your question** field.
7. Click **Save**.

Related topics

- Deleting inquiries about pending requests on page 126
- Answering inquiries about requests on page 134
- Submitting inquiries about escalated requests on page 150
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Deleting inquiries about pending requests

If your problem with the request has become irrelevant, you can recall your question. Once the question has been deleted, the request is taken off hold and all the original approvers can approve the request again.

To delete an inquiry

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending Attestations** page, in the list, click the request that you inquired about.
4. In the details pane, click **Recall last question**.

5. (Optional) In the **Recall last question** dialog, enter a reason for recalling the question.
6. Click **OK**.

Related topics

- Sending inquiries about pending requests on page 125
- Answering inquiries about requests on page 134
- Deleting inquiries about escalated requests on page 151
- Revoking hold status of pending requests on page 127
- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Revoking hold status of pending requests

Once an inquiry has been made about a request, it is given hold status in the approval workflow. Only the originator of the inquiry can make an approval decision about a request with hold status.

You can cancel the hold status using the following actions:

- Delete the inquiry (see Deleting inquiries about pending requests on page 126)
- Revoke the status after answering the question

To revoke a request's hold status after the inquiry has been answered

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Pending Requests**.
3. On the **Pending requests** page, in the list, click the request with the inquiry you want to answer.
4. In the details pane, click **Revoke hold status**.
5. In the **Revoke hold status** dialog, click **OK**.

   The request is taken off hold. This releases the request for approval and it can also be edited by other approvers.

Related topics

- Sending inquiries about pending requests on page 125
- Deleting inquiries about pending requests on page 126
- Answering inquiries about requests on page 134
- Revoking hold status of escalated requests on page 152

- My actions (page description) on page 873
- Pending attestations (page description) on page 875

Displaying request history

You can display the request history to obtain an overview of all the products that you have requested for yourself or other identities, or to see the status of a current request. You also can resubmit requests in the request history (see Resubmitting requests on page 128).

TIP: How you can display all the requests in the system as auditor, see Displaying all requests on page 135.

To display the request history

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Request History**.

   This opens the **Request History** page (see Request history (page description) on page 862).
3. (Optional) To control which requests are displayed, click **Advanced search** (see Request history (page description) on page 862). For example, this allows you to show just pending requests (no approval decision yet made).
4. (Optional) To display details of a request, click the request whose details you want to see.

Related topics

- Canceling requests on page 129
- My requests (page description) on page 856

Resubmitting requests

You can repeat requests that are already in the request history. You can repeat the following types of request:

- Requests for products that are not (no longer) assigned to you
- Canceled requests
- Multi-request resource requests

To resubmit a request

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Request History**.
3. On the **Request History** page, in the list, click on the product you want to request again.
4. In the details pane, click **Submit again**.
5. (Optional) In the **Submit request again** dialog, enter a reason for repeating the request.
6. Click **OK**.

   This adds the product to your shopping cart.
7. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

Related topics

- Displaying request history on page 128
- My requests (page description) on page 856
- Request history (page description) on page 862

Canceling requests

You can cancel requests for individual products that are not (yet) assigned and have not yet been through a complete request workflow.

You can cancel your own requests or those of other identities that report to you.

TIP: For more information about how you cancel pending requests as a product approver, see Canceling pending requests on page 125.

To cancel a request

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Edit Requests**.
3. (Optional) To cancel a request belonging to another identity, on the **Renew or Unsubscribe** page, perform the following actions.
   a. Next to **Requests for**, click **Change**.
   b. In the **Employee** dialog, click the identity with the request you want to cancel.
4. In the list, click the product with the request you want to cancel.
5. In the details pane, click **Cancel request**.

6. In the **Cancel request** dialog, enter a reason for the cancellation.
7. Click **OK**.

   This cancels the request.

Related topics

- Requesting products on page 86
- Canceling pending requests on page 125
- My requests (page description) on page 856
- Renewing or unsubscribing (page description) on page 865

Renewing products with limit validity periods

Some products are only valid for a limited period. You can renew products with a limited validity period that have already been assigned.

You can renew products for yourself or for other identities that you manage.

> NOTE: You are notified 14 days before your limited period products expire. You can renew the product after receiving this message. The products are automatically unsubscribed once they have expired.

To renew a product's validity period

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Edit Requests**.

   This opens the **Renew or Unsubscribe** page (see Renewing or unsubscribing (page description) on page 865) and displays all the products with and without limited validity periods.

   > TIP: To list the limited requests sequentially, click the **Valid until** column header.
3. (Optional) If you want to renew a product of another identity, perform the following actions:
   a. Next to **Requests for**, click **Change**.
   b. In the **Employee** dialog, click the identity with the product you want to renew.
4. Select the check box next to the product you want to renew.
5. Click **Renew**.
6. In the **Renew** dialog, perform one of the following actions:
   - Leave the **Valid until** field empty to the give the product unlimited availability.
   - To set the validity period, enter a date in the **Valid until** field.

7. (Optional) In the **Reason** field, enter a reason for changing the validity period.
8. Click **Save**.

   This triggers a new request with the changed validity period. After the request has been approved, the product's validity is changed with respect to your input.

Related topics

- Setting the validity period of products in your shopping cart on page 91
- My requests (page description) on page 856
- Renewing or unsubscribing (page description) on page 865

Unsubscribing products

You can unsubscribe from products that are already assigned if they are not longer required. Products that can be unsubscribed have the **Assigned** status.

You can unsubscribe your own products or those belonging to other identities that you manage.

To unsubscribe a product

1. In the menu bar, click **Request** > **My Requests**.
2. On the **My requests** page, click **Edit Requests**.

   This opens the **Renew or Unsubscribe** page (see Renewing or unsubscribing (page description) on page 865) and displays all the products that can be renewed or unsubscribed.
3. (Optional) If you want to unsubscribe a product of another identity, perform the following actions:
   a. Next to **Requests for**, click **Change**.
   b. In the **Employee** dialog, click the identity with the product you want to unsubscribe.
4. On the **Renew or Unsubscribed** page, click the product in the list that you want to unsubscribe.
5. Click **Unsubscribe**.
6. (Optional) In the **Unsubscribe** dialog, in the **Unsubscribed as from** field, enter the date for unsubscribing the product. If you leave this field empty, the product is unsubscribed once you have clicked **Saved**.
7. (Optional) In the **Reason** field, enter a reason for unsubscribing.
8. Click **Save**.

Related topics

- My requests (page description) on page 856
- Renewing or unsubscribing (page description) on page 865

Displaying approvals

You can display all approvals of product requests that you, or the identities that report to you, decided upon.

> TIP: How you, as auditor, can display all the approvals, see Displaying all approvals on page 136.

To display approvals

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Approval History**.

   This opens the **Approval History** page (see Approval history (page description) on page 881).
3. (Optional) Click **Advanced search** to control which approvals are display (see Approval history (page description) on page 881). For example, this allows you to show just pending requests (no approval decision yet made).

Related topics

- Withdrawing delegations from pending requests on page 121
- Removing additional approvers of pending requests on page 120
- Approving and denying requests on page 111
- Undoing approvals on page 132
- My actions (page description) on page 873
- Approval history

Undoing approvals

If you have made an approval decision about a request, you can undo the approval. To do this, the following prerequisites must be met:

- You made the last approval decision about the request.
- The last approval decision about the request was made at another approval level.
- There are no parallel approval steps at the current approval level.

To undo an approval

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Approval History**.
3. (Optional) To control which requests are displayed on the **Approval History** page, click **Advanced search** (see Approval history (page description) on page 881). For example, this allows you to show just pending requests (no approval decision yet made).
4. In the list, click the request whose the approval that you want to undo.
5. In the details pane, click **Revoke last decision**.
6. In the dialog, perform the following actions:
    a. In the **Reason for the recall**, enter why you want to undo the approval.
    b. Click **Revoke last decision**.

Related topics

- Displaying approvals on page 132
- My actions (page description) on page 873
- Approval history (page description) on page 881
- Request history (page description) on page 862

Request inquiries

Before a pending request case is approved, the approver can send you a question about it. You can display and respond to these inquiries.

Detailed information about this topic

- Displaying request inquiries on page 133
- Answering inquiries about requests on page 134
- Sending inquiries about pending requests on page 125
- Submitting inquiries about escalated requests on page 150
- Deleting inquiries about pending requests on page 126
- Deleting inquiries about escalated requests on page 151

Displaying request inquiries

You can see inquiries that have been made to you about a product request.

To display an inquiry

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Request inquiries**.

   This opens the **Request inquiries** page (see Request inquiries (page description) on page 883).
3. (Optional) Click an inquiry in the list.

   For more information, see the details pane.

Related topics

- Sending inquiries about pending requests on page 125
- Submitting inquiries about escalated requests on page 150
- My actions (page description) on page 873
- Request inquiries (page description) on page 883

Answering inquiries about requests

You can respond to inquiries that have been made to you about a product request.

To respond to inquiries

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Request inquiries**.
3. On the **Request inquiries** page, click the inquiry in the list that you want to answer.
4. In the details pane, click **Respond**.
5. In the **Respond to an inquiry** dialog, enter your answer in the **Your answer** field.
6. Click **Save**.

Related topics

- Sending inquiries about pending requests on page 125
- Submitting inquiries about escalated requests on page 150
- My actions (page description) on page 873
- Request inquiries (page description) on page 883

Auditing requests

As auditor, you can display the requests and approval decisions of all identities in the system.

Detailed information about this topic

- Displaying all requests on page 135
- Displaying all approvals on page 136

Displaying all requests

You can view all requests of all or only specific identities.

TIP: To find out how to display your own requests or requests placed by your identities, see Displaying request history on page 128.

To display all requests

1. In the menu bar, click **Request** > **Auditing**.
2. On the **Auditing** page, click **Request**.

   This opens the **Auditing - Requests** page (see Auditing – Requests (page description) on page 885).
3. (Optional) To control which requests are displayed (see Auditing – Requests (page description) on page 885), click (**Advanced search**). For example, you can display only pending (not yet assigned) requests.
4. (Optional) In the list, click a product request.

   For more information, see the details pane.

To display all request of a specific identity

1. In the menu bar, click **Request** > **Auditing**.
2. On the **Auditing** page, click **Request**.

   This opens the **Auditing - Requests** page (see Auditing – Requests (page description) on page 885).
3. Click **Advanced earch**.
4. In the **Advanced search** dialog, next to **Select identity**, click **Assign**.
5. In the **Employee** dialog, select the identity whose requests you want to display.
6. In the **Advanced search** dialog, click **Search**.
7. (Optional) Click **Advanced Search** to control which requests are displayed (see Auditing – Requests (page description) on page 885). For example, you can display

requests placed by the selected identity for other identities.

8. (Optional) In the list, click a product request.

   For more information, see the details pane.

Related topics

- Auditing (page description) on page 884
- Auditing – Requests (page description) on page 885

Displaying all approvals

You can display all approvals in which any or specific identities were involved.

TIP: To find out how to display your own approvals or approvals in which your identities were involved, see Displaying approvals on page 132.

To display all approvals

1. In the menu bar, click **Request** > **Auditing**.
2. On the **Auditing** page, click **Approval**.

   This opens the **Auditing - Approvals** page (see Auditing - Approvals (page description) on page 887).
3. (Optional) Click **Advanced Search** to control which requests are displayed (see Auditing - Approvals (page description) on page 887). For example, you can display only pending (not yet assigned) requests.
4. (Optional) In the list, click a product request.

   For more information, see the details pane.

To display all approvals of a specific identity

1. In the menu bar, click **Request** > **Auditing**.
2. On the **Auditing** page, click **Approval**.

   This opens the **Auditing - Approvals** page (see Auditing - Approvals (page description) on page 887).
3. Click **Advanced search**.
4. In the **Advanced search** dialog, next to **Select identity**, click **Assign**.
5. In the **Employee** dialog, select the identity whose approvals you want to display.
6. In the **Advanced search** dialog, click **Search**.
7. (Optional) Click **Advanced Search** to control which requests are displayed (see Auditing - Approvals (page description) on page 887). For example, you can display only pending (not yet assigned) requests.

8. (Optional) In the list, click a product request.

   For more information, see the details pane.

Related topics

- Auditing (page description) on page 884
- Auditing - Approvals (page description) on page 887

Escalated requests

If there are requests pending and the approver responsible is not available for an extended period or has no access to the Web Portal, you can make an approval decision about this request if you are the fallback approver or member of the chief approval team. For more detailed information about the chief approval team, see the One Identity Manager IT Shop Administration Guide. For more information about the **IT Shop escalation** page, see the IT Shop escalation (page description) on page 890.

Detailed information about this topic

- Escalating approvals of pending requests on page 122
- Displaying escalated requests on page 137
- Approving and denying escalated requests on page 138
- Appointing other approvers for escalated requests on page 145
- Changing priority of escalated requests on page 148
- Adding more products to escalated requests on page 149
- Canceling escalated requests on page 150
- Submitting inquiries about escalated requests on page 150
- Revoking hold status of escalated requests on page 152

Displaying escalated requests

If you are a fallback approver or a member of the chief approval team and identities escalate requests for products, you can display these requests. Then you can make approval decisions about the escalated requests (see Approving and denying escalated requests on page 138).

> TIP: For more information about escalating a pending request as approver, see Escalating approvals of pending requests on page 122.

To display escalated requests

1. In the menu bar, click **Request** > **Escalation**.

   This opens the **IT Shop Escalation** page (see IT Shop escalation (page description) on page 890).
2. (Optional) To limit the results to a specific requester, click **Assign** next to **Requester** and click an identity.
3. (Optional) To limit the results to a specific recipient, click **Assign** next to **Recipient** and click an identity.
4. (Optional) To limit the results to a specific request, click **Assign** next to **Request number** and click an identity.
5. (Optional) To limit the results to a specific product, click **Assign** next to **Product** and click an identity.

   This lists the requests according to your filter criteria.

Related topics

- Displaying pending requests on page 111
- IT Shop escalation (page description) on page 890

Approving and denying escalated requests

If an approver escalates the approval of a product request, you can grant or deny approval for this escalated request. If you approve a request, the product is available to the identity.

TIP: For more information about escalating a pending request as approver, see Escalating approvals of pending requests on page 122.

To make an approval decision about an escalated request

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. Perform one of the following actions:
   - To approve a request, click ☑ (**Approve**) next to the request.
   - To deny a request, click ☒ (**Deny**) next to the request.

   TIP: To grant or deny approval for all the requests displayed, click (**Approve all**) or (**Deny all**).
4. Click **Next**.
5. (Optional) On the **Pending Requests – Approvals** page, perform the following actions:

(Optional) On the **IT Shop Escalation - Approvals** page, perform the following actions:

- For approved requests:
  - To provide a reason for all approved requests, enter the reason in the **Reason for approvals** field.
  - To use a predefined standard reason for all approved requests, select the reason in the **Standard reason** list.
- For denied requests:
  - To provide a reason for all denied requests, enter the reason in the **Reason for approvals** field.
  - To use a predefined standard reason for all denied requests, select the reason in the **Standard reason** list.
- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

> TIP: By giving reasons, your approvals are more transparent and support the audit trail.

> NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

6. (Optional) To specify the validity period for a requested product, perform the following actions:
   a. In the list, in the **Valid from** column, click on a value.
   b. In the **Valid from** dialog, specify from when the product is valid.
   c. Click **Close**.
   d. In the list, in the **Valid until** column, click on a value.
   e. In the **Valid until** dialog, specify until when the product is valid.
7. Click **Save**.

Related topics

- Approving and denying requests on page 111
- Displaying and approving entire requests of escalated requests on page 140
- Approving escalated requests from newly created Active Directory groups on page 141
- Approving escalated requests from newly created SharePoint groups on page 142
- Approving new manager's escalated assignments on page 144
- IT Shop escalation (page description) on page 890

Displaying and approving entire requests of escalated requests

You can see all other products of an escalated product request that are included in this request (meaning, they were sent in the same shopping cart). You can approve pending requests together.

To display an entire request and approve all the requests contained in it.

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, mark the product with the request you want to see in its entirety.
4. In the details pane, click **more** > **Show entire request**.
5. On the **Request overview** page, click **Approve all**.
6. On the **IT Shop escalation - Approvals** page, perform the following actions:
    - To provide a reason for all request approvals, enter the reason in the **Reason for approvals** field.
    - To use a predefined standard reason for all request approvals, select the reason in the **Standard reason**.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
7. (Optional) To specify the validity period for a requested product, perform the following actions:
    a. In the list, in the **Valid from** column, click on a value.
    b. In the **Valid from** dialog, specify from when the product is valid.
    c. Click **Close**.
    d. In the list, in the **Valid until** column, click on a value.
    e. In the **Valid until** dialog, specify until when the product is valid.
8. Click **Save**.

Related topics

- Displaying and approving entire requests of pending requests on page 113
- IT Shop escalation (page description) on page 890

- Requests overview (page description) on page 893
- IT Shop escalation - Approvals (page description) on page 894

Approving escalated requests from newly created Active Directory groups

Identities can create Active Directory groups by requesting the **New Active Directory security group** or the **New Active Directory distribution group** product. As approver, you can make approval decisions about requests like this. If you approve the request, you must provide additional information about the group.

To approve a request to create a new Active Directory group

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the request for the new Active Directory group.
4. In the details pane, click **Configure the new group**.
5. In the dialog, enter additional information about the new group:
   - **Name**: Enter a name for the group.
   - **Group scope**: Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can select one of the following group scopes:
     - **Global group**: Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group’s domain.
     - **Local**: Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.
     - **Universal**: Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
   - **Container**: Click **Assign**/**Change** and select a container for the group.
6. Click **OK**.
7. Next to the request, click ☑ (**Approve**).
8. Click **Next**.
9. On the **IT Shop escalation - Approvals** page, perform the following actions:

- To provide a reason for all request approvals, enter the reason in the **Reason for approvals** field.
- To use a predefined standard reason for all request approvals, select the reason in the **Standard reason**.
- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

10. (Optional) To specify the validity period for a requested product, perform the following actions:
    a. In the list, in the **Valid from** column, click on a value.
    b. In the **Valid from** dialog, specify from when the product is valid.
    c. Click **Close**.
    d. In the list, in the **Valid until** column, click on a value.
    e. In the **Valid until** dialog, specify until when the product is valid.
11. Click **Save**.

Related topics

- Requesting new Active Directory groups on page 104
- Approving pending requests from newly created Active Directory groups on page 114
- IT Shop escalation (page description) on page 890
- IT Shop escalation - Approvals (page description) on page 894

Approving escalated requests from newly created SharePoint groups

Identities can create SharePoint groups by requesting the **New SharePoint group** product. As approver, you can make approval decisions about requests like this. If you approve the request, you must provide additional information about the group.

To approve a request to create a new SharePoint group

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the request for the new SharePoint group.

4. In the details pane, click **Enter information for the new group**.
5. In the dialog, enter additional information about the new group:
    - **Site collection**: Select a site collection where the group will be applied. A site collection groups sites together. User account and their access permissions are managed on the sites.
    - **Display name**: Enter a name for the new group.
    - **Description**: Enter a description for the SharePoint group.
6. Click **OK**.
7. Next to the request, click ☑ (**Approve**).
8. Click **Next**.
9. On the **IT Shop escalation - Approvals** page, perform the following actions:
    - To provide a reason for all request approvals, enter the reason in the **Reason for approvals** field.
    - To use a predefined standard reason for all request approvals, select the reason in the **Standard reason**.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. (Optional) To specify the validity period for a requested product, perform the following actions:
    a. In the list, in the **Valid from** column, click on a value.
    b. In the **Valid from** dialog, specify from when the product is valid.
    c. Click **Close**.
    d. In the list, in the **Valid until** column, click on a value.
    e. In the **Valid until** dialog, specify until when the product is valid.
11. Click **Save**.

Related topics

- Requesting new SharePoint groups on page 106
- Approving pending requests from newly created SharePoint groups on page 116
- IT Shop escalation (page description) on page 890
- IT Shop escalation - Approvals (page description) on page 894

Approving new manager's escalated assignments

Managers can allocate new managers for their identities. To do this, they must select the new manager and a deadline in the future for changing managers (see Assigning other managers to my identities on page 299). An assignment of this type triggers a request of type **New manager assignment**.

You can cancel entitlements already assigned to the identity on the given date.

To approve an escalated assignment of a new manager

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the **New manager assignment** request.
4. In the details pane, click **Show the identity's entitlements**.
5. (Optional) If the identity has already been assigned entitlements or products, these will be removed or unsubscribed by default on the effective date. If you want the identity to retain these entitlements or products when transferring to the new manager, in the **New manager assignment** dialog, disable the check boxes next to the respective entitlements and products.
6. Click **Save**.
7. Next to the request, click ☑ (**Approve**).
8. Click **Next**.
9. On the **IT Shop escalation - Approvals** page, perform the following actions:
    - To provide a reason for all request approvals, enter the reason in the **Reason for approvals** field.
    - To use a predefined standard reason for all request approvals, select the reason in the **Standard reason**.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. (Optional) To specify from when the new manager is responsible for the identity, perform the following:
    a. Click **Valid from**.
    b. In the **Valid from** field in the dialog, enter the date from which you want the new manager to take over.

    c. Click **Close**.
11. Click **Save**.

Related topics

- Assigning other managers to my identities on page 299
- Approving new managers' pending requests on page 117
- IT Shop escalation (page description) on page 890
- IT Shop escalation - Approvals (page description) on page 894

Appointing other approvers for escalated requests

You can give an another identity the task of approving a product request. To do this, you have the following options:

- Reroute approval
  You give the task of approving to another approval level (see Rerouting escalated requests' approvals on page 145).
- Appoint additional approver
  You can give an another identity the task of approving (see Appointing additional approvers to escalated requests on page 146). The additional approver must make an approval decision in addition to the other approvers.
  The additional approver can reject the approval and return it to you (see Rejecting request approval on page 122).
  You can withdraw an additional approver. For example, if the other approver is not available.
- Delegate approval
  You delegate the task of approving to another approval level (see Delegating approvals of escalated requests to other identities on page 147). This identity is added as approver in the current approval step and makes approval decisions on your behalf.
  The new approver can reject the approval and return it to you (see Rejecting request approval on page 122).
  You can withdraw a delegation and delegate another identity. For example, if the other approver is not available.

Rerouting escalated requests' approvals

You can let another approval level of the approval workflow make the approval decision about a product. For example, if approval is required by a manager in a one-off case.

To reroute an approval

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the request whose the approval that you want to reroute.
4. In the details pane, click **more** > **Reroute approval**.
5. In the **Reroute approval** dialog next to the approval level that you want to reroute to, click **Reroute approval**.
6. (Optional) In the dialog, enter a reason for rerouting.
7. Click **Reroute approval**.

Related topics

- Rerouting approvals of pending requests on page 119
- IT Shop escalation (page description) on page 890

Appointing additional approvers to escalated requests

You can give another identity the task of approving a product request. The additional approver must make an approval decision in addition to the other approvers.

To add an additional approver

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. Click the request in the list that you want to add another approver to.
4. In the details pane, click **more** > **Add approver**.
5. In the **Select additional approver** dialog, click the identity you want to act as an additional approver.
6. In the dialog, enter a reason for adding the additional approver.
7. Click **Save**.

Related topics

- Removing additional approvers from escalated requests on page 147
- Appointing additional approvers to pending requests on page 120
- IT Shop escalation (page description) on page 890

Removing additional approvers from escalated requests

If you have given the task of approving a product request to another identity, you can remove this additional approver as long as the product has the status **Request**. Once the additional approver has been removed, the original approvers are the only approvers for this request and you can add a new additional approver.

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the request to which you added an additional approver.
4. In the details pane, click **Withdraw additional approval**.
5. In the dialog, enter a reason for withdrawing the approver.
6. Click **Save**.

Related topics

- Appointing additional approvers to escalated requests on page 146
- Removing additional approvers of pending requests on page 120
- IT Shop escalation (page description) on page 890

Delegating approvals of escalated requests to other identities

You can delegate an approval decision about a request to another identity. You can revoke this action in the approval history (see Withdrawing delegations from escalated requests on page 148).

To delegate an approval

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the request whose approval decision you want to delegate to another identity.
4. In the details pane, click **more** > **Delegate approval**.
5. In the **Select an identity that is allowed to approve** dialog, click the identity to which you want delegate the approval.
6. In the dialog, enter a reason for the delegation.
7. Click **Save**.

Related topics

- Withdrawing delegations from escalated requests on page 148
- Delegating approvals of pending requests to other identities on page 121
- IT Shop escalation (page description) on page 890

Withdrawing delegations from escalated requests

If a request's approval has been delegated to another identity, you can withdraw the delegation.

To withdraw an approval delegation

1. In the menu bar, click **Request** > **My Actions**.
2. On the **My Actions** page, click **Approval History**.
3. On the **Approval History** page, in the list, click the request with the approval delegation you want to withdraw.
4. In the details pane, click **Withdraw delegation**.
5. In the dialog, enter a reason why you are withdrawing the approval delegation.
6. Click **Save**.

Related topics

- Delegating approvals of escalated requests to other identities on page 147
- Withdrawing delegations from pending requests on page 121
- My actions (page description) on page 873
- Approval history (page description) on page 881

Changing priority of escalated requests

As an approver of requests, you can set the priority of individual requests. For example, this positions requests at different positions in the request list. This means that if the list is sorted in descending order, requests with high priority are listed at the top.

To change a request's priority

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the request with the priority that you want to change.
4. In the details pane, click **more** > **Change priority**.

5. In the **Set the priority for this request** dialog, in the **Priority** menu, click the priority you want to use for this request.
6. Click **Apply**.
7. Then make an approval decision about the request (see Approving and denying escalated requests on page 138).

   NOTE: The modified priority is not changed until you have saved you approval decision about the request.

Related topics

- Approving and denying escalated requests on page 138
- Changing priority of pending requests on page 123
- IT Shop escalation (page description) on page 890

Adding more products to escalated requests

You can add more products to requests.

To add more products to a request

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the request to which want to add products to.
4. In the details pane, click **more** > **Show entire request**.
5. On the **Request overview** page, click **Add items to this request**.
6. On the **Request** page, add the product you want to the shopping cart, edit the products in the shopping cart and send the request.

Related topics

- Adding products to the shopping cart on page 87
- Managing products in the shopping cart on page 88
- Submitting requests on page 97
- Displaying and approving entire requests of escalated requests on page 140
- Adding more products to pending requests on page 124
- IT Shop escalation (page description) on page 890
- Requests overview (page description) on page 893
- Request (page description) on page 858

Canceling escalated requests

As approver, you can cancel a request. This cancels the request and the requested product is not assigned to the recipient but it can be requested again.

TIP: To find out how to cancel requests for yourself or for identities that you manage, see Canceling requests on page 129.

To cancel an escalated request

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, mark the request that you want to cancel.
4. In the details pane, click **Withdraw request**.
5. In the **Withdraw request** dialog, enter a reason for the cancellation.
6. Click **OK**.

Related topics

- Canceling requests on page 129
- Canceling pending requests on page 125
- IT Shop escalation (page description) on page 890

Submitting inquiries about escalated requests

Before you make an approval decision about a request, you can send a question to an identity about it.

NOTE: Once an inquiry has been made about a request, it is given hold status in the approval workflow. Only the originator of the inquiry (or the chief approval team) can make an approval decision about a request with hold status. You can revoke hold status with the following actions:

- Delete the inquiry (see Deleting inquiries about escalated requests on page 151)
- Revoke the status after answering the question (see Revoking hold status of escalated requests on page 152)

To make an inquiry

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. On the **IT Shop Escalation Approval** page, click the request in the list that you want to inquire about.
4. In the details pane, click **more** > **Send inquiry**.
5. In the **Submit an inquiry about this request** dialog, click the identity to which you want send the inquiry.
6. In the **Submit an inquiry about this request** dialog, enter your question in the **Your question** field.
7. Click **Save**.

Related topics

- Deleting inquiries about escalated requests on page 151
- Answering inquiries about requests on page 134
- Sending inquiries about pending requests on page 125
- IT Shop escalation (page description) on page 890

Deleting inquiries about escalated requests

If your problem with the request has become irrelevant, you can recall your question. Once the question has been deleted, the request is taken off hold and all the original approvers can approve the request again.

To delete an inquiry

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the request that you inquired about.
4. In the details pane, click **Recall last question**.
5. (Optional) In the **Recall last question** dialog, enter a reason for recalling the question.
6. Click **OK**.

Related topics

- Submitting inquiries about escalated requests on page 150
- Answering inquiries about requests on page 134
- Deleting inquiries about pending requests on page 126
- Revoking hold status of escalated requests on page 152
- IT Shop escalation (page description) on page 890

Revoking hold status of escalated requests

Once an inquiry has been made about a request, it is given hold status in the approval workflow. Only the originator of the inquiry can make an approval decision about a request with hold status.

You can cancel the hold status using the following actions:

- Delete the inquiry (see Deleting inquiries about escalated requests on page 151)
- Revoke the status after answering the question

To revoke a request's hold status after the inquiry has been answered

1. In the menu bar, click **Request** > **Escalation**.
2. On the **IT Shop escalation** page, apply a filter to limit the results to a specific requester, specific recipient or a specific request (see Displaying escalated requests on page 137).
3. In the list, click the request with the inquiry you want to answer.
4. In the details pane, click **Revoke hold status**.
5. In the **Revoke hold status** dialog, click **OK**.

   The request is taken off hold. This releases the request for approval and it can also be edited by other approvers.

Related topics

- Submitting inquiries about escalated requests on page 150
- Deleting inquiries about escalated requests on page 151
- Answering inquiries about requests on page 134
- Revoking hold status of pending requests on page 127
- IT Shop escalation (page description) on page 890

4

Attestation

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. The same workflow is used for attestation and recertification.

There are attestation policies defined for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom. Once attestation starts, attestation cases are created that contain all the necessary information about the attestation objects and the attestor. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Attestors for attestation cases on page 163
- Sending attestation reminders on page 167
- My attestation cases on page 175
- Pending attestations on page 177
- Displaying attestation history on page 188
- Attestation inquiries on page 189
- Auditing attestations on page 190
- Managing attestations on page 154
- Escalation on page 192

Managing attestations

You can define attestation policies for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom. Once attestation is started, attestation cases are created that contain all the necessary information about the attestation objects and the attestor. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

TIP: The attestation statistics provide you with an overview of your company's attestations. For more information, see What statistics are available? on page 800.

Detailed information about this topic

- Attestation policies on page 154
- Attestation runs on page 160

Attestation policies

You can define attestation policies for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.

Detailed information about this topic

- Displaying attestation policies on page 154
- Setting up attestation policies on page 156
- Editing attestation policies on page 157
- Copying attestation policies on page 158
- Deleting attestation policies on page 160
- Appendix: Attestation conditions and approval policies from attestation procedures on page 808

Displaying attestation policies

You can display enabled and disabled attestation policies.

To display attestation polices

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Settings**.

This opens the **Attestation Policy Settings** page (see Managing attestation policy (page description) on page 978).

3. (Optional) To display disabled attestation policies, on the **Attestation Policy Settings** page, enable the **Show disabled policies** option.

Related topics

- Displaying attestation policies main data on page 155
- Displaying attestation policies statistics on page 155
- Governance administration (page description) on page 975
- Managing attestation policy (page description) on page 978

Displaying attestation policies main data

To obtain an overview of an attestation policy, you can display its main data.

To display main data of an attestation policy

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Settings**.
3. (Optional) To display disabled attestation policies, on the **Attestation Policy Settings** page, enable the **Show disabled policies** option.
4. Next to the attestation policy whose main data you want to show, click (**Edit attestation policy**).

   This opens the **Edit attestation policy** page (see Editing attestation policies (page description) on page 982).
5. (Optional) To display the objects that fulfill the conditions, perform one of the following actions:
   - Objects that fulfill one condition: Under **Object selection**, click the number link next to the condition in the **Matching objects** column.
   - Objects that fulfill all conditions: Under **Object selection**, click the number link at the end of the list of conditions.

Related topics

- Governance administration (page description) on page 975
- Managing attestation policy (page description) on page 978
- Editing attestation policies (page description) on page 982

Displaying attestation policies statistics

You can obtain more information about attestation policies by display their statistics.

To display attestation policy statistics

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Settings**.
3. (Optional) To display disabled attestation policies, on the **Attestation Policy Settings** page, enable the **Show disabled policies** option.
4. In the row containing the attestation policy whose statistics you want to see, click (**Edit attestation policy**).

   This opens the **Edit attestation policy** page (see Editing attestation policies (page description) on page 982).
5. Click the **Statistics** tab.

Related topics

- Governance administration (page description) on page 975
- Managing attestation policy (page description) on page 978
- Editing attestation policies (page description) on page 982

Setting up attestation policies

To fulfill new regulation requirements, you can create new attestation policies.

To create a new attestation policy

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Settings**.
3. On the **Attestation Policy Settings** page, click **New attestation policy**.
4. On the **Attestation Policy Settings** page, enter the new attestation policy's main data (see Creating new attestation policies (page description) on page 979).

   NOTE: The attestation procedure you select when you create a new attestation policy is important. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The available options are modified to match the attestation procedure.
5. To specify which objects to attest, under **Object selection**, click (**Add**).
6. In the **Edit condition** dialog, in the **Condition type** menu, click the condition type to use (see Appendix: Attestation conditions and approval policies from attestation procedures on page 808).

   NOTE: The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.
7. (Optional) Depending on which condition type you have selected, you can filter the selection of objects to attest (see Appendix: Attestation conditions and approval policies from attestation procedures on page 808).

8. Click **OK**.
9. (Optional) Create more conditions if required. To do this, click (**Add**).
10. (Optional) If you have specified more than one condition, you must specify whether one or all of the conditions must be fulfilled by enabling the appropriate option:
    - **All conditions must be fulfilled**: The next time the attestation policy is run, new attestation cases are added for all objects fulfilling all of the conditions. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.
    - **At least one condition must be fulfilled**: The next time the attestation policy is run, new attestation cases are added for all objects that fulfill at least one of the conditions. Use of this option generates a superset of all the individual conditions of the selected objects.
11. Click **Create**.

Related topics

- Appendix: Attestation conditions and approval policies from attestation procedures on page 808
- Governance administration (page description) on page 975
- Managing attestation policy (page description) on page 978
- Creating new attestation policies (page description) on page 979

Editing attestation policies

For example, you can modify attestation policies to include more conditions.

To edit an attestation policy

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Settings**.
3. On the **Attestation Policy Settings** page, next to the attestation policy you want to edit, click **Edit attestation policy**.

    TIP: To show disabled attestation policies, enable the **Include deactivated policies**.

    NOTE: The system contains default attestation policies. These policies can only be edited to a limited degree. If you want to make changes to a default attestation policy, create a copy and edit the copy (see Copying attestation policies on page 158).
4. For more information, see Setting up attestation policies on page 156.
5. To specify which objects to attest, perform one of the following actions:

- To add a new condition, under **Object selection** click (**Add**).
- To edit an existing condition, under **Object selection**, click (**Edit**).
- To delete an existing condition, click (**Delete condition**).

6. In the **Edit condition** dialog, in the **Condition type** menu, click the condition type to use (see Appendix: Attestation conditions and approval policies from attestation procedures on page 808).

   NOTE: The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.

7. (Optional) Depending on which condition type you have selected, you can filter the selection of objects to attest (see Appendix: Attestation conditions and approval policies from attestation procedures on page 808).
8. Click **OK**.
9. (Optional) Create or modify more conditions if required. To do this, click (**Add**).
10. (Optional) If you have specified more than one condition, you must specify whether one or all of the conditions must be fulfilled by enabling the appropriate option:
    - **All conditions must be fulfilled**: The next time the attestation policy is run, new attestation cases are added for all objects fulfilling all of the conditions. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.
    - **At least one condition must be fulfilled**: The next time the attestation policy is run, new attestation cases are added for all objects that fulfill at least one of the conditions. Use of this option generates a superset of all the individual conditions of the selected objects.
11. Click **Save**.

Related topics

- Appendix: Attestation conditions and approval policies from attestation procedures on page 808
- Governance administration (page description) on page 975
- Managing attestation policy (page description) on page 978
- Editing attestation policies (page description) on page 982

Copying attestation policies

You can copy existing attestation policies and then edit them. For example, if you want to make changes to a default attestation policy, you can copy it, edit the copy, and then use it.

Copied attestation policies can be deleted again.

To copy an attestation policy

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Settings**.
3. On the **Attestation Policy Settings** page, next to the attestation policy you want to copy, click **Copy attestation policy**.

   TIP: To show disabled attestation policies, enable the **Include deactivated policies**.
4. Confirm the prompt with **Yes** in the dialog.
5. For more information, see Setting up attestation policies on page 156.
6. To specify which objects to attest, perform one of the following actions:
   - To add a new condition, under **Object selection** click (**Add**).
   - To edit an existing condition, under **Object selection**, click (**Edit**).
   - To delete an existing condition, click (**Delete condition**).
7. In the **Edit condition** dialog, in the **Condition type** menu, click the condition type to use (see Appendix: Attestation conditions and approval policies from attestation procedures on page 808).

   NOTE: The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.
8. (Optional) Depending on which condition type you have selected, you can filter the selection of objects to attest (see Appendix: Attestation conditions and approval policies from attestation procedures on page 808).
9. Click **OK**.
10. (Optional) Create or modify more conditions if required. To do this, click (**Add**).
11. (Optional) If you have specified more than one condition, you must specify whether one or all of the conditions must be fulfilled by enabling the appropriate option:
    - **All conditions must be fulfilled**: The next time the attestation policy is run, new attestation cases are added for all objects fulfilling all of the conditions. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.
    - **At least one condition must be fulfilled**: The next time the attestation policy is run, new attestation cases are added for all objects that fulfill at least one of the conditions. Use of this option generates a superset of all the individual conditions of the selected objects.
12. Click **Create**.

Related topics

- Appendix: Attestation conditions and approval policies from attestation procedures on page 808
- Governance administration (page description) on page 975

- Managing attestation policy (page description) on page 978
- Editing attestation policies (page description) on page 982

Deleting attestation policies

You can delete attestation policies that are not used anymore.

> NOTE: You can only delete attestation policies if no attestation cases are associated with it anymore.

To delete an attestation policy

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Settings**.
3. (Optional) To show disabled attestation policies, on the **Attestation Policy Settings** page, select the **Show disabled policies** check box.
4. On the **Manage Attestation Policies** page, click (**Delete Attestation Policy**) next to the attestation policy you want to delete.
5. In the dialog, confirm the prompt with **Yes**.

Related topics

- Governance administration (page description) on page 975
- Managing attestation policy (page description) on page 978

Attestation runs

Once attestation has started, a corresponding attestation run is added that, in turn, creates an attestation case. Attestation runs show you the attestation prediction and give you an overview of pending attestation cases.

Detailed information about this topic

- Displaying attestation policy runs on page 161
- Displaying attestation cases of application runs on page 161
- Extending attestation runs on page 162
- Sending reminders about attestation runs on page 174

Displaying attestation policy runs

You can the display attestation runs of attestation policies. In addition, you can query further details for each attestation run, such as general data, attestation details, and the attestation prediction.

To display attestation policy runs

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation runs**.

   This opens the **Attestation Policy Runs** page (see Attestation runs (page description) on page 976)
3. (Optional) To control which attestation runs are displayed, next to **Min. category**, click one of the options (see Attestation runs).
4. (Optional) To display more details of an attestation run (current date, details about attestation, attestation prediction, and attestors), click the attestation run in the list, then the information is displayed in the details pane.

Related topics

- Sending reminders about attestation runs on page 174
- Governance administration (page description) on page 975
- Attestation runs (page description) on page 976

Displaying attestation cases of application runs

You can view all attestation cases created in an attestation run. In addition, you can approve or reject pending attestation cases.

To display attestation cases of an attestation run

1. In the menu bar, click **Attestation** > **Attestation runs**.
2. On the **Attestation Runs** page, click **Details** next to the attestation run with the attestation cases you want to display.
3. In the **View Attestation Run Details** pane, click the **Attestation cases** tab.
4. (Optional) To further limit the attestation cases to be displayed, click (**Filter**) on the **Attestation cases** tab.
5. (Optional) To approve or deny an attestation case, perform the following actions in the **Attestation cases** tab:
   a. Select the check box next to the attestation case that you want to approve or deny.
   b. Click **Approve** or **Deny**.

c. In the **Approve Attestation Case/Deny Attestation Case** pane, enter a reason for your approval decision in the **Reason for decision** field.

d. Click **Save**.

6. (Optional) To view more details of an attestation case, click **Details** next to the attestation case and refer to the **View Attestation Case Details** pane for the relevant information.

Related topics

- Displaying pending attestation cases on page 178
- Granting or denying attestation cases on page 179

Extending attestation runs

You can extend attestation runs.

To extend an attestation run

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation runs**.
3. On the **Attestation Policy Runs** page, click the attestation run that you want to extend.
4. In the details pane, click **Extend attestation run**.
5. In dialog's **New due date** field, enter a new due date.
6. In the **Reason** field, enter a reason for extending.
7. Click **OK**.

Related topics

- Sending reminders about attestation runs on page 174
- Governance administration (page description) on page 975
- Attestation runs (page description) on page 976

Attestation by peer group analysis

Using peer group analysis, approval for attestation cases can be granted or denied automatically. For example, a peer group might be all identities in the same department. Peer group analysis assumes that these identities require the same products. For example, if the majority of identities belonging to a department have a particular product, assignment to another identity in the department can be approved automatically. This helps to accelerate approval processes.

Peer group analysis can be used during attestation of the following memberships:

- Assignments of system entitlements to user accounts
- Secondary memberships in business roles

All identities that have the same manager or that belong to the same primary or secondary division as the identity linked to the attestation object (= identity to be attested) are grouped together as a peer group.

For more information about peer group analysis, see the *One Identity Manager Attestation Administration Guide*.

Related topics

- Appendix: Attestation conditions and approval policies from attestation procedures on page 808

Attestors for attestation cases

You can display the identities that still have pending attestation cases to approve. To do this, you have the following options:

- You can display all the attestation cases that affect you (see Displaying attestors of my attestation cases on page 163).
- You can display all the attestation cases that you can approve (see Displaying attestors of pending attestation cases on page 164).
- You can display attestors for attestation cases through the attestation history (see Displaying attestors of pending attestation cases through the attestation history on page 165).
- You can display attestors for attestation cases that will be audited (see Displaying attestors of pending auditing attestation cases on page 166).
- You can display attestors for escalated attestation cases (see Displaying attestors of escalated attestation cases on page 166).

Displaying attestors of my attestation cases

You can display identities that still have attestation cases to approve that affect you.

To show attestors of an attestation case

1. In the menu bar, click **Attestation** > **My Attestation Status**.
2. (Optional) On the **My Attestation Status** page, click on a tab to display the corresponding attestation cases.
3. In the list, click the attestation case that has attestors you want to show.
4. In the details pane, click **Actions** > **Send a reminder mail**.

The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Attestation** > **My Attestation Status**.
2. (Optional) On the **My Attestation Status** page, click on a tab to display the corresponding attestation cases.
3. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve that affect you. You can now send these identities a reminder.

Related topics

- Sending attestation reminders on page 167
- My attestation status (page description) on page 897

Displaying attestors of pending attestation cases

You can see identities that still have pending attestation cases that you can also approve.

To show attestors of an attestation case

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
   - To display a specific object, click on the corresponding tile and then the object.
   - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. In the list, click the attestation case that has attestors you want to show.
6. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:

- To display a specific object, click on the corresponding tile and then the object.
- To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.

4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Sending attestation reminders on page 167
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Displaying attestors of pending attestation cases through the attestation history

You can see identities that still have pending attestation cases by using the attestation history.

To show attestors of an attestation case

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Attestation History**.
3. On the **Attestation History** page, in the list, click the attestation case (status: **pending**) that has the attestors you want to display.
4. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Attestation History**.
3. Click **View approvers for pending cases**.

   You can now send these identities a reminder.

Related topics

- Sending attestation reminders on page 167
- My actions (page description) on page 899
- Attestation history (page description) on page 971

Displaying attestors of pending auditing attestation cases

You can see identities for attestation cases that will be audited.

To show attestors of an attestation case

1. In the menu bar, click **Attestation** > **Auditing**.
2. On the **Auditing** page, in the list, click the attestation case (status: **pending**) that has the attestors you want to display.
3. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Attestation** > **Auditing**.
2. Click **View approvers for pending cases**.

   You can now send these identities a reminder.

Related topics

- Sending attestation reminders on page 167
- Auditing (page description) on page 974

Displaying attestors of escalated attestation cases

You can see identities that still have escalated attestation cases to approve.

To show attestors of an attestation case

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the escalated attestation case you want to see.
3. On the **Attestation escalation - <attestation policy name>** page, in the list, click the attestation case to see its attestors.
4. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the escalated attestation case you want to see.
3. Click **View approvers for pending cases**.

   You can now send these identities a reminder.

Related topics

- Sending attestation reminders on page 167
- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

Sending attestation reminders

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

- You can send reminders to attestors of attestation cases that affect you (see Sending reminders for your own attestation cases on page 168).
- You can send reminders to attestors of attestation cases that you can approve (see Sending reminders about pending attestation cases on page 169).
- You can send reminders to attestors of attestation cases about attestation history (see Sending reminders of pending attestation cases through the attestation history on page 171).
- You can send reminders to attestors of attestation cases that will be audited (see Sending reminders of pending auditing attestation cases on page 172).
- You can send reminders to attestors of escalated attestation cases (see Sending reminders about escalated attestation cases on page 173).

- You can send reminders to attestors of attestation cases that belong to certain attestation runs (see Sending reminders about attestation runs on page 174).

Sending reminders for your own attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestation that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Attestation** > **My Attestation Status**.
2. (Optional) On the **My Attestation Status** page, click on a tab to display the corresponding attestation cases.
3. In the list, click the attestation case that has attestors you want to remind.
4. In the details pane, click **Actions** > **Send a reminder mail**.
5. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
6. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
7. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Attestation** > **My Attestation Status**.
2. (Optional) On the **My Attestation Status** page, click on a tab to display the corresponding attestation cases.
3. Click **Send reminder**.
4. In the **Send a reminder mail** dialog, enter the message for the attestor.
5. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Attestation** > **My Attestation Status**.
2. (Optional) On the **My Attestation Status** page, click on a tab to display the corresponding attestation cases.
3. Click **View approvers for pending cases**.
4. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
5. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
6. Edit the email and send it to the attestor.

Related topics

- Attestors for attestation cases on page 163
- My attestation status (page description) on page 897

Sending reminders about pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestation that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
   - To display a specific object, click on the corresponding tile and then the object.
   - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.

4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. In the list, click the attestation case that has attestors you want to remind.
6. In the details pane, click **Actions** > **Send a reminder mail**.
7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
8. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. On the **Pending Attestations** page, click the appropriate tile and then the object with the attestation cases you want to see.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. Click **Send reminder**.
6. In the **Send a reminder mail** dialog, enter the message for the attestor.
7. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
   - To display a specific object, click on the corresponding tile and then the object.
   - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. Click **View approvers for pending cases**.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Attestors for attestation cases on page 163
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Sending reminders of pending attestation cases through the attestation history

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can show all the attestation that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 2).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Attestation History**.
3. On the **Attestation History** page, in the list, click the attestation case (status: **pending**) that has the attestors you want to send a reminder to.
4. In the details pane, click **Actions** > **Send a reminder mail**.
5. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
6. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
7. Edit the email and send it to the attestor.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Attestation History**.
3. On the **Attestation History** page, click **View attestors for pending attestation cases**.
4. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
5. Select the email program that you want to use.

This opens an email template with the attestor's email address.

6. Edit the email and send it to the attestor.

Related topics

- Attestors for attestation cases on page 163
- My actions (page description) on page 899
- Attestation history (page description) on page 971

Sending reminders of pending auditing attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can show all the attestation that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 2).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Attestation** > **Auditing**.
2. On the **Auditing** page, in the list, click the attestation case (status: **pending**) that has the attestors you want to send a reminder to.
3. In the details pane, click **Actions** > **Send a reminder mail**.
4. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
5. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
6. Edit the email and send it to the attestor.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Attestation** > **Auditing**.
2. On the **Auditing** page, click **View attestors for pending attestation cases**.
3. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
4. Select the email program that you want to use.

This opens an email template with the attestor's email address.

5. Edit the email and send it to the attestor.

Related topics

- Attestors for attestation cases on page 163
- Auditing (page description) on page 974

Sending reminders about escalated attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can show all the attestation that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 2).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the escalated attestation case you want to see.
3. On the **Pending Attestations** page, in the list, click the attestation case that has the attestors you want to send a reminder to.
4. In the details pane, click **Actions** > **Send a reminder mail**.
5. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
6. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
7. Edit the email and send it to the attestor.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the escalated attestation case you want to see.
3. On the **Pending Attestation** page, click **View attestors for pending attestation cases**.

4. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
5. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
6. Edit the email and send it to the attestor.

Related topics

- Attestors for attestation cases on page 163
- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

Sending reminders about attestation runs

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

To send a reminder to all attestors of all attestation runs

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation runs**.
3. On the **Attestation Policy Runs** page, click **Remind attestors of ALL visible runs**.
4. (Optional) In the **Send reminder mail** dialog, enter a message for the attestors. This message is added to the reminder.
5. Click **Send reminder**.

To send a reminder to attestors of a selected attestation run

1. In the menu bar, click **Attestation** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation runs**.
3. On the **Attestation Runs** page, click the attestation run that has the attestors you want to remind.
4. Perform one of the following actions:
   - To send a reminder to all attestors of the attestation run, click **Send reminder** in the details pane.
   - To send a reminder to specific attestors of the attestation run, in the details pane, click the **Attestors** tab, select the check boxes in front of the corresponding attestors and click **Send reminder**.
5. (Optional) In the **Send reminder mail** dialog, enter a message for the attestors. This message is added to the reminder.
6. Click **Send reminder**.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 975
- Attestation runs (page description) on page 976

My attestation cases

In the Web Portal, the attestation cases that affect you are displayed separately on the **My Attestation Status** page For more information about the **My Attestation Status** page, see My attestation status (page description) on page 897.

Detailed information about this topic

- Displaying your attestation cases on page 175
- Displaying attestors of my attestation cases on page 163
- Sending reminders for your own attestation cases on page 168
- Granting or denying my attestation cases on page 176

Displaying your attestation cases

You can see all the attestation cases that affect you. In addition, you can obtain more information about the attestation cases.

To display your own attestation cases

1. In the menu bar, click **Attestation** > **My Attestation Status**.

   This opens the **My Attestation Status** page (see My attestation status (page description) on page 897)
2. (Optional) On the **My Attestation Status** page, click on a tab to display the corresponding attestation cases.
3. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. Click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.

d. (Optional) Click **View current state of the object**

   This opens an overview in shapes of the attestation.

4. (Optional) To display all the identities that can approve an attestation case, perform the following actions:
   a. Click the attestation case.
   b. In the details pane, click the **Workflow** tab.
5. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Displaying pending attestation cases on page 178
- Displaying all attestation cases on page 191
- Displaying escalated attestation cases on page 192
- Attestors for attestation cases on page 163
- Sending attestation reminders on page 167
- My attestation status (page description) on page 897

Granting or denying my attestation cases

If you have sufficient permission, you can grant or deny approval for attestation cases that affect you.

To approve an attestation case

1. In the menu bar, click **Attestation** > **My Attestation Status**.
2. On the **My Attestation Status** page, click**Approve**.
3. On the **Pending Attestations – Identity** page, click on a tab to display the corresponding attestation cases.
4. Perform one of the following actions:
   - To approve an attestation case, click (**Approve**) next to the attestation case.
   - To deny an attestation case, click (**Deny**) next to the attestation case.

   TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).

5. Click **Next**.
6. (Optional) On the **Pending Attestations – Approvals** page, perform the following actions:
   - For approved attestation case:
     - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
   - For denied attestation cases:
     - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
   - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

   TIP: By giving reasons, your approvals are more transparent and support the audit trail.

   NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
7. Click **Save**.

Related topics

- Granting or denying attestation cases on page 179
- Granting or denying escalated attestation cases on page 194
- My attestation status (page description) on page 897
- Pending attestations – approvals (page description) on page 970

Pending attestations

Attestation policies are run on a schedule and generate attestation cases. As attestor, you can verify attestation cases and make approval decisions. Verifying attestations requires reading reports or manually checking objects that are being attested.

Detailed information about this topic

- Displaying pending attestation cases on page 178
- Granting or denying attestation cases on page 179
- Appointing other approvers for pending attestation cases on page 180

- Rejecting approval of attestation cases on page 184
- Submitting inquiries about pending attestation cases on page 185
- Revoking the hold status of pending attestation cases on page 187

Displaying pending attestation cases

As attestor, you can see the attestation cases that still require approval. In addition, you can obtain more information about the attestation cases.

To display pending attestation cases

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
   - To display a specific object, click on the corresponding tile and then the object.
   - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. Click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
6. (Optional) To display all the identities that can approve an attestation case, perform the following actions:
   a. Click the attestation case.
   b. In the details pane, click the **Workflow** tab.
7. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Displaying your attestation cases on page 175
- Displaying all attestation cases on page 191
- Displaying escalated attestation cases on page 192
- Attestors for attestation cases on page 163
- Sending attestation reminders on page 167
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Granting or denying attestation cases

As attestor, you can grant or deny approval for attestation cases under your supervision.

To approve an attestation case

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
    - To display a specific object, click on the corresponding tile and then the object.
    - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. Perform one of the following actions:
    - To approve an attestation case, click (**Approve**) next to the attestation case.
    - To deny an attestation case, click (**Deny**) next to the attestation case.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
6. Click **Next**.
7. (Optional) On the **Pending Attestations – Approvals** page, perform the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.

- To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
- For denied attestation cases:
  - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
  - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

8. Click **Save**.

Related topics

- Granting or denying my attestation cases on page 176
- Granting or denying escalated attestation cases on page 194
- My actions (page description) on page 899
- Pending attestations (page description) on page 899
- Pending attestations – approvals (page description) on page 970

Appointing other approvers for pending attestation cases

You can give an additional identity the task of approving an attestation case. To do this, you have the following options:

- Reroute approval
  You give the task of approving to another approval level (see Rerouting approvals of pending attestation cases on page 181).
- Appoint additional approver
  You can give an another identity the task of approving Appointing additional approvers to pending attestation cases on page 182). The additional approver must make an approval decision in addition to the other approvers.
  The additional approver can reject the approval and return it to you (see Rejecting approval of attestation cases on page 184).
  You can withdraw an additional approver. For example, if the other approver is not available.
- Delegate approval
  You delegate the task of approving to another approval level (see Delegating

approvals of pending attestation cases to other identities on page 183). This identity is added as approver in the current approval step and makes approval decisions on your behalf.
The new approver can reject the approval and return it to you (see Rejecting approval of attestation cases on page 184).
You can withdraw a delegation and delegate another identity. For example, if the other approver is not available.

Rerouting approvals of pending attestation cases

You can let another approval level of the approval workflow make the approval decision about an attestation case. For example, if approval is required by a manager in a one-off case.

To reroute an approval

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
    - To display a specific object, click on the corresponding tile and then the object.
    - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. On the **Pending Attestations** page, click the attestation case whose approval you want to reroute.
6. In the details pane, click **Actions** > **Reroute approval**.
7. In the **Reroute approval** dialog next to the approval level that you want to reroute to, click **Reroute approval**.
8. (Optional) In the dialog, enter a reason for rerouting.
9. Click **Reroute approval**.

Related topics

- Rerouting approvals of escalated attestation cases on page 195
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Appointing additional approvers to pending attestation cases

You can give an another identity the task of approving an attestation case. The additional approver must make an approval decision in addition to the other approvers.

To add an additional approver

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
   - To display a specific object, click on the corresponding tile and then the object.
   - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. On the **Pending Attestations** page, click the attestation case to which you want to add an additional approver.
6. In the details pane, click **Actions** > **Add approver**.
7. In the **Select additional approver** dialog, click the identity you want to act as an additional approver.
8. In the dialog, enter a reason for adding the additional approver.
9. Click **Save**.

Related topics

- Removing additional approvers from pending attestation cases on page 182
- Appointing additional approvers to escalated attestation cases on page 196
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Removing additional approvers from pending attestation cases

If you have given the task of approving an attestation case to another identity, you can remove this additional approver as long as the attestation case has **pending** status. Once the additional approver has been removed, the original approvers are the only approvers for this attestation case and you can add a new additional approver.

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.

3. (Optional) On the **Pending attestations** page, perform one of the following actions:
   - To display a specific object, click on the corresponding tile and then the object.
   - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. On the **Pending Attestations** page, click the attestation case to which you added an additional approver.
6. In the details pane, click **Withdraw additional approval**.
7. In the dialog, enter a reason for withdrawing the approver.
8. Click **Save**.

Related topics

- Appointing additional approvers to pending attestation cases on page 182
- Removing additional approvers from escalated attestation cases on page 196
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Delegating approvals of pending attestation cases to other identities

You can delegate an approval decision about an attestation case to another identity. You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).

To delegate an approval

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
   - To display a specific object, click on the corresponding tile and then the object.
   - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. On the **Pending Attestation** page, click the attestation case whose approval decision you want to delegate to another identity.
6. In the details pane, click **Actions** > **Delegate approval**.

7. In the **Select an identity that is allowed to approve** dialog, click the identity to which you want delegate the approval.
8. In the dialog, enter a reason for the delegation.
9. Click **Save**.

Related topics

- Withdrawing delegations from pending attestation case approvals on page 184
- Delegating approvals of escalated attestation cases to other identities on page 197
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Withdrawing delegations from pending attestation case approvals

If an attestation's approval has been delegated to another identity, you can withdraw the delegation.

To withdraw an approval delegation

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Attestation History**.
3. On the **Attestation History** page, click the request whose approval delegation you want to withdraw.
4. In the details pane, click **Withdraw delegation**.
5. In the dialog, enter a reason why you are withdrawing the approval delegation.
6. Click **Save**.

Related topics

- Delegating approvals of pending attestation cases to other identities on page 183
- Withdrawing delegations from escalated attestation case approvals on page 198
- My actions (page description) on page 899
- Attestation history (page description) on page 971

Rejecting approval of attestation cases

If you have been added to an attestation case as an additional approver the approval of the attestation case was passed to you, you can reject the approval and return the attestation case to the original approver.

To reject an approval

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
   - To display a specific object, click on the corresponding tile and then the object.
   - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. On the **Pending Attestations** page, in the list, click the attestation case that you do not want to make an approval decision about.
6. In the details pane, click **Actions** > **Reject approval**.
7. In the dialog, enter a reason for the rejecting.
8. Click **Save**.

Related topics

- Appointing additional approvers to escalated requests on page 146
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Submitting inquiries about pending attestation cases

Before you make an approval decision about an attestation case, you can send a question to an identity about it.

NOTE: Once an inquiry has been made about a n attestation case, it is given hold status in the approval workflow. Only the originator of the inquiry (or the chief approval team) can make an approval decision about an attestation case with hold status. You can revoke hold status with the following actions:

- Delete the inquiry (see Deleting inquiries about pending attestation cases on page 186)
- Revoke the status after answering the question (see Revoking the hold status of pending attestation cases on page 187)

To make an inquiry

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.

3. (Optional) On the **Pending attestations** page, perform one of the following actions:
    - To display a specific object, click on the corresponding tile and then the object.
    - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. On the **Pending Attestations**, in the list, click the attestation case that you want to inquire about.
6. In the details pane, click **Actions** > **Send inquiry**.
7. In the **Submit an inquiry about this attestation case** dialog, click the identity to which you want send the inquiry.
8. In the **Submit an inquiry about this attestation case** dialog box, enter your question in the **Your question** field.
9. Click **Save**.

Related topics

- Deleting inquiries about pending attestation cases on page 186
- Answering attestation case inquiries on page 190
- Submitting inquiries about escalated attestation cases on page 198
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Deleting inquiries about pending attestation cases

If your problem with the request has become irrelevant, you can recall your question. Once the question has been deleted, the request is taken off hold and all the original approvers can approve the request again.

To delete an inquiry

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
    - To display a specific object, click on the corresponding tile and then the object.
    - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.

5. On the **Pending Attestations** page, click the attestation case in the list that you inquired about.
6. In the details pane, click **Recall last question**.
7. (Optional) In the **Recall last question** dialog, enter a reason for recalling the question.
8. Click **OK**.

Related topics

- Submitting inquiries about pending attestation cases on page 185
- Answering attestation case inquiries on page 190
- Deleting inquiries about escalated attestation cases on page 199
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Revoking the hold status of pending attestation cases

Once an inquiry has been made about an attestation case, it is given hold status in the approval workflow. Only the originator of the inquiry can make an approval decision about an attestation case with hold status.

You can cancel the hold status using the following actions:

- Delete the inquiry (see Deleting inquiries about pending attestation cases on page 186)
- Revoke the status after answering the question

To revoke an attestation case's hold status after the inquiry has been answered

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Pending Attestations**.
3. (Optional) On the **Pending attestations** page, perform one of the following actions:
    - To display a specific object, click on the corresponding tile and then the object.
    - To display attestation cases by attestation policies, click **Switch to policy view** and then the attestation policy.
4. (Optional) On the **Pending Attestations** page, click on a tab to display the corresponding attestation cases.
5. On the **Pending Attestation** page, click the attestation in the list with the inquiry that was answered.
6. In the details pane, click **Revoke hold status**.

7. In the **Revoke hold status** dialog, click **OK**.

   The request is taken off hold. This releases the request for approval and it can also be edited by other approvers.

Related topics

- Submitting inquiries about pending attestation cases on page 185
- Deleting inquiries about pending attestation cases on page 186
- Answering attestation case inquiries on page 190
- My actions (page description) on page 899
- Pending attestations (page description) on page 899

Displaying attestation history

You can obtain an overview of all the attestation cases relevant to you or identities that report to you, by displaying the attestation history.

To display the attestation history

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Attestation History**.

   This opens the **Attestation History** page (see Attestation history (page description) on page 971).
3. (Optional) To filter which attestation cases are displayed, select or deselect the check boxes next to **Attestation state**. For example, this allows you to show just pending attestation cases (no approval decision yet made).
4. (Optional) To display details of an attestation case, click the attestation case whose details you want to display.
5. (Optional) To show an object involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
6. (Optional) To display all the identities that can approve the attestation case, perform the following actions:

a. In the list, click the attestation case.
b. In the details pane, click the **Workflow** tab.

7. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Withdrawing delegations from pending attestation case approvals on page 184
- My actions (page description) on page 899
- Attestation history (page description) on page 971

Attestation inquiries

Before an attestation case is approved, the approver can send you a question about this attestation case. You can show the inquiry and answer it.

Detailed information about this topic

- Displaying attestation case inquiries on page 189
- Answering attestation case inquiries on page 190
- Submitting inquiries about pending attestation cases on page 185
- Submitting inquiries about escalated attestation cases on page 198
- Deleting inquiries about pending attestation cases on page 186
- Deleting inquiries about escalated attestation cases on page 199

Displaying attestation case inquiries

You can see inquiries that have been made to you about an attestation case.

To display an inquiry

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Attestation Inquiries**.

   This opens the **Attestation Inquiries** page (see Attestation inquiries (page description) on page 973).

3. (Optional) Click an inquiry in the list.

   For more information, see the details pane.

Related topics

- Submitting inquiries about pending attestation cases on page 185
- Submitting inquiries about escalated attestation cases on page 198
- My actions (page description) on page 899
- Attestation inquiries (page description) on page 973

Answering attestation case inquiries

You can respond to inquiries that have been made to you about an attestation case.

To respond to inquiries

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Attestation Inquiries**.
3. On the **Attestation inquiries** page, click the inquiry in the list that you want to answer.
4. In the details pane, click **Respond**.
5. In the **Respond to an inquiry** dialog, enter your answer in the **Your answer** field.
6. Click **Save**.

Related topics

- Submitting inquiries about pending attestation cases on page 185
- Submitting inquiries about escalated attestation cases on page 198
- My actions (page description) on page 899
- Attestation inquiries (page description) on page 973

Auditing attestations

As auditor, you can display all the attestation cases (already approved or not approved and pending) in the system.

Detailed information about this topic

- Displaying all attestation cases on page 191
- Displaying attestors of pending auditing attestation cases on page 166

Displaying all attestation cases

You can see all attestation cases. At the same time you can decide whether you only want to show attestation cases with a certain status (approved, denied, pending) or those of a specific attestors. In addition, you can obtain more information about the attestation cases.

TIP: For more information about how you display your own attestation cases or pending attestation cases, see Displaying your attestation cases on page 175 and Displaying pending attestation cases on page 178.

To display all attestation cases

1. In the menu bar, click **Attestation** > **Auditing**.
2. (Optional) On the **Auditing** page, next to **Attestor**, click **Assign** and select the identity whose attestation cases you want to view.
3. (Optional) To further limit or delimit the attestation cases to view, check the appropriate boxes next to **Attestation status** (see Auditing (page description) on page 974). For example, this allows you to show just pending attestation cases (no approval decision yet made).
4. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
    a. Click the attestation case.
    b. In the details pane, click **Show details**.
    c. In the **Attested object** dialog, select an object in the **Object** menu.

       This shows information about the object.
    d. (Optional) Click **View current state of the object**

       This opens an overview in shapes of the attestation.
5. (Optional) To display all the identities that can approve an attestation case, perform the following actions:
    a. Click the attestation case.
    b. In the details pane, click the **Workflow** tab.
6. (Optional) To show previous attestation cases for the selected object, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click the **History** tab.

This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Displaying your attestation cases on page 175
- Displaying pending attestation cases on page 178
- Displaying escalated attestation cases on page 192
- Attestors for attestation cases on page 163
- Sending attestation reminders on page 167
- Auditing (page description) on page 974

Escalation

If the are attestations pending and the approver responsible is not available for an extended period or has no access to Web Portal, the fallback approver or member of the chief approval team must make an approval decision. For more information about the chief approval team, see the One Identity Manager Attestation Administration Guide.

> IMPORTANT: The two-person principle can be broken for attestations because chief approval team members can make approval decisions about attestation cases at any time.

Detailed information about this topic

- Displaying escalated attestation cases on page 192
- Granting or denying escalated attestation cases on page 194
- Submitting inquiries about escalated attestation cases on page 198
- Revoking the hold status of escalated attestation cases on page 200

Displaying escalated attestation cases

You can see escalated attestation cases. In addition, you can obtain more information about the attestation cases.

To view escalated attestation cases

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the attestation case you want to see.

This opens the **Attestation Escalation Approval – Attestation policy** page (see Attestation escalation approval – Attestation policy (page description) on page 985).

3. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
    a. Click the attestation case.
    b. In the details pane, click **Show details**.
    c. In the **Attested object** dialog, select an object in the **Object** menu.
       This shows information about the object.
    d. (Optional) Click **View current state of the object**
       This opens an overview in shapes of the attestation.
4. (Optional) To display all the identities that can approve an attestation case, perform the following actions:
    a. Click the attestation case.
    b. In the details pane, click the **Workflow** tab.
5. (Optional) To show previous attestation cases for the selected object, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click the **History** tab.
       This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Displaying your attestation cases on page 175
- Displaying pending attestation cases on page 178
- Displaying all attestation cases on page 191
- Attestors for attestation cases on page 163
- Sending attestation reminders on page 167
- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

Granting or denying escalated attestation cases

To approve an attestation case

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the attestation case you want to see.
3. Perform one of the following actions:
   - To approve an attestation case, click ☑ (**Approve**) next to the attestation case.
   - To deny an attestation case, click ☒ (**Deny**) next to the attestation case.

   TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
4. Click **Next**.
5. (Optional) On the **Attestation Escalation Approval** page, perform the following actions:
   - For approved attestation case:
     - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
   - For denied attestation cases:
     - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
   - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

   TIP: By giving reasons, your approvals are more transparent and support the audit trail.

   NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
6. Click **Save**.

Related topics

- Granting or denying my attestation cases on page 176
- Granting or denying attestation cases on page 179
- Attestation escalation approval (page description) on page 984

- Pending attestations (page description) on page 899
- Attestation escalation approval – Attestation policy (page description) on page 985
- Attestation escalation – Approvals (page description) on page 988

Appointing other approvers for escalated attestation cases

You can give an additional identity the task of approving an attestation case. To do this, you have the following options:

- Reroute approval
  You give the task of approving to another approval level (see Rerouting approvals of escalated attestation cases on page 195).
- Appoint additional approver
  You can give an another identity the task of approving (see Appointing additional approvers to escalated attestation cases on page 196). The additional approver must make an approval decision in addition to the other approvers.
  The additional approver can reject the approval and return it to you (see Rejecting approval of attestation cases on page 184).
  You can withdraw an additional approver. For example, if the other approver is not available.
- Delegate approval
  You delegate the task of approving to another approval level (see Delegating approvals of escalated attestation cases to other identities on page 197). This identity is added as approver in the current approval step and makes approval decisions on your behalf.
  The new approver can reject the approval and return it to you (see Rejecting approval of attestation cases on page 184).
  You can withdraw a delegation and delegate another identity. For example, if the other approver is not available.

Rerouting approvals of escalated attestation cases

You can let another approval level of the approval workflow make the approval decision about an attestation case. For example, if approval is required by a manager in a one-off case.

To reroute an approval

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the attestation case you want to see.
3. On the **Pending Attestations** page, click the attestation case whose approval you want to reroute.

4. In the details pane, click **Actions** > **Reroute approval**.
5. In the **Reroute approval** dialog next to the approval level that you want to reroute to, click **Reroute approval**.
6. (Optional) In the dialog, enter a reason for rerouting.
7. Click **Reroute approval**.

Related topics

- Rerouting approvals of pending attestation cases on page 181
- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

Appointing additional approvers to escalated attestation cases

The additional approver must make an approval decision in addition to the other approvers.

To add an additional approver

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the attestation case you want to see.
3. On the **Pending Attestations** page, click the attestation case to which you want to add an additional approver.
4. In the details pane, click **Actions** > **Add approver**.
5. In the **Select additional approver** dialog, click the identity you want to act as an additional approver.
6. In the dialog, enter a reason for adding the additional approver.
7. Click **Save**.

Related topics

- Removing additional approvers from escalated attestation cases on page 196
- Appointing additional approvers to pending attestation cases on page 182
- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

Removing additional approvers from escalated attestation cases

If you have given the task of approving an attestation case to another identity, you can remove this additional approver as long as the attestation case has **pending** status. Once the additional approver has been removed, the original approvers are the only approvers for this attestation case and you can add a new additional approver.

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the attestation case you want to see.
3. On the **Pending Attestations** page, click the attestation case to which you added an additional approver.
4. In the details pane, click **Withdraw additional approval**.
5. In the dialog, enter a reason for withdrawing the approver.
6. Click **Save**.

Related topics

- Appointing additional approvers to escalated attestation cases on page 196
- Removing additional approvers from pending attestation cases on page 182
- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

Delegating approvals of escalated attestation cases to other identities

You can delegate an approval decision about an attestation case to another identity. You can revoke this action in the attestation history (see Withdrawing delegations from escalated attestation case approvals on page 198).

To delegate an approval

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the attestation case you want to see.
3. On the **Pending Attestation** page, click the attestation case whose approval decision you want to delegate to another identity.
4. In the details pane, click **Actions** > **Delegate approval**.
5. In the **Select an identity that is allowed to approve** dialog, click the identity to which you want delegate the approval.
6. In the dialog, enter a reason for the delegation.
7. Click **Save**.

Related topics

- Withdrawing delegations from escalated attestation case approvals on page 198
- Delegating approvals of pending attestation cases to other identities on page 183
- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

Withdrawing delegations from escalated attestation case approvals

If an attestation's approval has been delegated to another identity, you can withdraw the delegation.

To withdraw an approval delegation

1. In the menu bar, click **Attestation** > **My Actions**.
2. On the **My Actions** page, click **Attestation History**.
3. On the **Attestation History** page, click the request whose approval delegation you want to withdraw.
4. In the details pane, click **Withdraw delegation**.
5. In the dialog, enter a reason why you are withdrawing the approval delegation.
6. Click **Save**.

Related topics

- Delegating approvals of escalated attestation cases to other identities on page 197
- Withdrawing delegations from pending attestation case approvals on page 184
- My actions (page description) on page 899
- Attestation history (page description) on page 971

Submitting inquiries about escalated attestation cases

Before you make an approval decision about an attestation case, you can send a question to an identity about it.

NOTE: Once an inquiry has been made about a n attestation case, it is given hold status in the approval workflow. Only the originator of the inquiry (or the chief approval team) can make an approval decision about an attestation case with hold status. You can revoke hold status with the following actions:

- Delete the inquiry (see Deleting inquiries about escalated attestation cases on page 199)
- Revoke the status after answering the question (see Revoking the hold status of escalated attestation cases on page 200)

To make an inquiry

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the attestation case you want to see.

3. On the **Pending Attestations**, in the list, click the attestation case that you want to inquire about.
4. In the details pane, click **Actions** > **Send inquiry**.
5. In the **Submit an inquiry about this attestation case** dialog, click the identity to which you want send the inquiry.
6. In the **Submit an inquiry about this attestation case** dialog box, enter your question in the **Your question** field.
7. Click **Save**.

Related topics

- Deleting inquiries about escalated attestation cases on page 199
- Answering attestation case inquiries on page 190
- Submitting inquiries about pending attestation cases on page 185
- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

Deleting inquiries about escalated attestation cases

If your problem with the request has become irrelevant, you can recall your question. Once the question has been deleted, the request is taken off hold and all the original approvers can approve the request again.

To delete an inquiry

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the attestation case you want to see.
3. On the **Pending Attestations** page, click the attestation case in the list that you inquired about.
4. In the details pane, click **Recall last question**.
5. (Optional) In the **Recall last question** dialog, enter a reason for recalling the question.
6. Click **OK**.

Related topics

- Submitting inquiries about escalated attestation cases on page 198
- Answering attestation case inquiries on page 190
- Deleting inquiries about pending attestation cases on page 186

- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

Revoking the hold status of escalated attestation cases

Once an inquiry has been made about an attestation case, it is given hold status in the approval workflow. Only the originator of the inquiry can make an approval decision about an attestation case with hold status.

You can cancel the hold status using the following actions:

- Delete the inquiry (see Deleting inquiries about escalated attestation cases on page 199)
- Revoke the status after answering the question

To revoke an attestation case's hold status after the inquiry has been answered

1. In the menu bar, click **Attestation** > **Escalation**.
2. On the **Attestation Escalation Approval** page, click the attestation policy of the attestation case you want to see.
3. On the **Pending Attestation** page, click the attestation in the list with the inquiry that was answered.
4. In the details pane, click **Revoke hold status**.
5. In the **Revoke hold status** dialog, click **OK**.

   The request is taken off hold. This releases the request for approval and it can also be edited by other approvers.

Related topics

- Submitting inquiries about escalated attestation cases on page 198
- Deleting inquiries about escalated attestation cases on page 199
- Answering attestation case inquiries on page 190
- Attestation escalation approval (page description) on page 984
- Attestation escalation approval – Attestation policy (page description) on page 985

5

Compliance

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information. For more information, see What statistics are available? on page 800.

Managing rule violations

Compliance rules that are violated generate rule violations. Rule violations can be granted or denied exception approval.

Detailed information about this topic

- Displaying approvable rule violations on page 202
- Granting and denying rule violation exceptions on page 202
- Resolving rule violations on page 204
- Displaying rule violation history on page 205

Displaying approvable rule violations

You can display rule violations that you can approve. In doing so, you can additionally display rule violations that have already have an approval decision.

To display rule violations

1. In the menu bar, click **Compliance** > **My Actions**.
2. On the **My Actions** page, click **Pending Rule Violations**.

   This opens the **Pending Rule Violations** page (see Pending rule violations (page description) on page 992) and displays all rule violations for which no approval decision has yet been made.
3. (Optional) To display rule violations that have already been approved or denied, click (**Reset filter: decision status**).
4. (Optional) To display details of the identity involved in a rule violation, take the following actions:
   a. In the list, click the rule violation.
   b. In the details pane, click the identity's name.

Related topics

- Displaying my identities' rule violations on page 302
- Displaying all rule violations on page 208
- Displaying approvable policy violations on page 206
- My actions (page description) on page 991
- Pending rule violations (page description) on page 992

Granting and denying rule violation exceptions

As exception approver, you can grant or deny exception approval to rule violations.

To make an approval decision about a rule violation

1. In the menu bar, click **Compliance** > **My Actions**.
2. On the **My Actions** page, click **Pending Rule Violations**.
3. On the **Pending Rule Violations** page, perform one of the following actions:
   - To grant an exception for a rule violation, click (**Grant exception**).
   - To deny an exception for a rule violation, click (**Deny exception**).
4. (Optional) To set an approval deadline, perform the following actions:
   a. In the list, click the role violation for which you want to set an approval deadline.
   b. In the details pane, enter the **Valid until** date.
5. Click **Next**.
6. (Optional) On the **Exception Approvals** page, perform the following actions:
   - For exceptions granted:
     - To provide a reason for all granted exceptions, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all granted exceptions, select the reason in the **Standard reason** list.
   - For exceptions denied:
     - To provide a reason for all denied exceptions, enter the reason in the **Reason for denials** field.
     - To use a predefined standard reason for all denied exceptions, select the reason in the **Standard reason** list.
   - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

   TIP: By giving reasons, your approvals are more transparent and support the audit trail.

   NOTE: For more detailed information about standard reasons, see the One Identity Manager Compliance Rules Administration Guide.
7. Click **Save**.

Related topics

- My actions (page description) on page 991
- Pending rule violations (page description) on page 992
- Exception approvals (page description) on page 993

Resolving rule violations

You can resolve compliance rule violations that you manage. Rule violations are caused by permissions, so you have the option to remove permissions when you want to resolve one.

Permission assignments play and important role when editing rule violations. For example, permissions assigned through a dynamic role cannot be removed.

The following consequences may result from removing permissions:

Table 22: Removing assigned permissions

Assignment Method	Removing the Entitlement
Direct assignment	Direct assignment is deleted when the entitlement is removed.
Inherited assignment	In the case of inherited permissions, there is an option provided to withdraw role membership from the identity.
Dynamic assignment	Permissions assigned through a dynamic role cannot be removed.
Assignment by request	If permissions were assigned through a request, the request ends if the permissions are removed.
Primary assignment	If permissions were assigned through a primary membership, the identity of the primary membership can be optionally revoked if the permissions are removed.

To resolve a rule violation

1. In the menu bar, click **Compliance** > **My Actions**.
2. On the **My Actions** page, click **Pending Rule Violations**.
3. On the **Pending rule violations** page, click the rule violation you would like to resolve.
4. In the details pane, click **Resolve**.

   This opens the **Resolve a rule violation** dialog and with more details about the rule violation and the permissions that lead to the rule violation.
5. Select the check box next to the permission that you want to be revoked.
6. Click **Next**.
7. In the **Verify** step, check the changes to be made.

   TIP: The **Action** column show the consequences of revoking.
8. Click **Next**.

9. In the **Loss of entitlements** step, check which permissions are to be revoked to avoid losing permissions accidentally.
10. Click **Next**.

    All permissions that were displayed for resolving the rule violation are withdrawn from the identity.

Related topics

- My actions (page description) on page 991
- Pending rule violations (page description) on page 992

Displaying rule violation history

To monitor your approval decisions about rule violations, you can see the approval decisions.

To display the rule violations history

1. In the menu bar, click **Compliance** > **My Actions**.
2. On the **My Actions** page, click **Rule Violation History**.

   This opens the **Rule Violation History** page (see Rule Violation History (page description) on page 994).

Related topics

- Displaying policy violation history on page 207
- My actions (page description) on page 991
- Rule Violation History (page description) on page 994

Managing policy violations

Policies that are violated generate policy violations. Policy violations may be approved as an exception. Policy violations that you can approve are displayed on the **Pending Policy Violations** page (see Pending policy violations (page description) on page 995).

Detailed information about this topic

- Displaying approvable policy violations on page 206
- Granting and denying rule violation exceptions on page 202
- Displaying policy violation history on page 207

Displaying approvable policy violations

You can display rule violations that you can approve. In doing so, you can additionally display policy violations that have already have an approval decision.

To display policy violations

1. In the menu bar, click **Compliance** > **My Actions**.
2. On the **My Actions** page, click **Pending Policy Violations**.

   This opens the **Pending Policy Violations** page (see Pending policy violations (page description) on page 995) and displays all policy violations for which no approval decision has yet been made.
3. (Optional) To display policy violations that have already been approved or denied, click **(Reset filter: decision status)**.

Related topics

- Displaying approvable rule violations on page 202
- Displaying all policy violations on page 208
- My actions (page description) on page 991
- Pending policy violations (page description) on page 995

Approving and denying policy violations

As exception approver, you can grant or deny exception approval to rule violations.

To make an approval decision about a rule violation

1. In the menu bar, click **Compliance** > **My Actions**.
2. On the **My Actions** page, click **Pending Rule Violations**.
3. On the **Pending Rule Violations** page, perform one of the following actions:
   - To grant an exception for a rule violation, click (**Grant exception**).
   - To deny an exception for a rule violation, click (**Deny exception**).
4. (Optional) To set an approval deadline, perform the following actions:
   a. In the list, click the role violation for which you want to set an approval deadline.
   b. In the details pane, enter the **Valid until** date.
5. Click **Next**.
6. (Optional) On the **Exception Approvals** page, perform the following actions:

- For exceptions granted:
    - To provide a reason for all granted exceptions, enter the reason in the **Reason for approvals** field.
    - To use a predefined standard reason for all granted exceptions, select the reason in the **Standard reason** list.
- For exceptions denied:
    - To provide a reason for all denied exceptions, enter the reason in the **Reason for denials** field.
    - To use a predefined standard reason for all denied exceptions, select the reason in the **Standard reason** list.
- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager Compliance Rules Administration Guide.

7. Click **Save**.

Related topics

- My actions (page description) on page 991
- Pending rule violations (page description) on page 992
- Exception approvals (page description) on page 993

Displaying policy violation history

To monitor your approval decisions about policy violations, you can see the approval decisions.

To display the policy violations history

1. In the menu bar, click **Compliance** > **My Actions**.
2. On the **My Actions** page, click **Policy Violation History**.

   This opens the **Policy Violation History** page (see Policy violations (page description) on page 998).

Related topics

- Displaying rule violation history on page 205
- My actions (page description) on page 991
- Policy violations (page description) on page 998

Auditing rule and policy violations

As auditor, you can display all the rule and policy violations (approved or pending) in the system.

Detailed information about this topic

- Displaying all rule violations on page 208
- Displaying all policy violations on page 208

Displaying all rule violations

You can display all rule violations. In addition, you can obtain more information about the rule violations.

To display all rule violations

1. In the menu bar, click **Compliance** > **Auditing**.
2. On the **Auditing** page, click **Rule Violations**.

   The **Auditing - Rule Violations** page opens (see Auditing - rule violations (page description) on page 999).
3. (Optional) To display only approvals from a specific identity, click **Assign** next to **Select approver** and select the identity.
4. (Optional) To display details of the identity involved in a rule violation, take the following actions:
   a. In the list, click the rule violation.
   b. In the details pane, click the identity's name.

Related topics

- Displaying approvable rule violations on page 202
- Auditing (page description) on page 998
- Auditing - rule violations (page description) on page 999

Displaying all policy violations

NOTE: This function is only available if the Company Policies Module or Compliance Rules Module is installed.

Here you can see all the policy violations. In addition, you can obtain more information about the policy violations.

To display all policy violations

1. In the menu bar, click **Compliance** > **Auditing**.
2. On the **Auditing** page, click **Policy Violations**.

   The **Auditing - Policy Violations** page opens (see Auditing – Policy violations (page description) on page 1000).

Related topics

- Displaying approvable policy violations on page 206
- Auditing (page description) on page 998
- Auditing – Policy violations (page description) on page 1000

Compliance – Governance Administration

The Web Portal provides you with comprehensive functionality for administrative management of compliance rules and company policies.

Detailed information about this topic

- Risk assessment on page 209
- Displaying compliance frameworks on page 212
- Displaying high risk objects on page 800
- Displaying compliance rules and rule violations on page 213
- Displaying reports about compliance rules and rule violations on page 214
- Displaying company policies and violations on page 215
- Displaying reports about company policies and violations on page 215
- Displaying compliance rules with SAP functions on page 216
- Displaying rule violations of identities with critical SAP functions on page 217

Risk assessment

Everyone with IT system authorization in a company represents a security risk for that company. For example, a person with permission to edit financial data in SAP carries a higher risk than an employee with permission to edit their own personal data. To quantify the risk, you can enter a risk value for every company resource in One Identity Manager. A risk index is calculated from this value for every person who is assigned this company resource, directly, or indirectly. Company resources include target system entitlements (for example, Active Directory groups or SAP profiles), system roles, subscribable reports, software, and resources. In this way, all the people that represent a particular risk to the company can be found.

In the context of Identity Audit, compliance rules can also be given a risk index. Each rule violation can increase the security risk. Therefore, these risk indexes are also included in the employee's risk calculation. You can define appropriate countermeasures through mitigating controls, and store them with the compliance rules.

Other factors can influence the calculation of employee risk indexes. These include: the type of resource assignment (approved request or direct assignment), attestations, exception approvals for rule violations, identity's responsibilities, and defined weightings. Furthermore, the risk index can be calculated for all business roles, organizations, and system roles that have company resources assigned to them. The user account risk index is calculated based on the system entitlements assigned.

For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Detailed information about this topic

- Displaying risk index functions on page 210
- Editing risk index functions on page 210
- Enabling/disabling risk index functions on page 211

Displaying risk index functions

You can display risk index functions that contribute to the calculation of the risk index of all assigned company resources.

To display all risk index functions

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Runs**.

   This opens the **Risk Assessment** page (see Risk assessment (page description)).

Related topics

- Governance administration (page description) on page 1001
- Risk assessment (page description)

Editing risk index functions

You can edit risk index functions that contribute to the calculation of the risk index of all assigned company resources.

To edit a risk index function

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Runs**.
3. On the **Risk Assessment** page, in the list, click the risk index function that you want to edit.
4. In dialog, from the **Calculation type** menu, select the calculation type that you want to use for calculating the risk index.
    - **Maximum (weighted)**: The highest value from all relevant risk indexes is determined, weighted and used as the basis for further calculation.
    - **Maximum (normalized)**: The highest value from all relevant risk indexes is calculated, weighted with the normalized weighting factor and taken as basis for the next calculation.
    - **Increment**: The risk index of table column (target) is incremented by a fixed value. This value is specified in **Weighting/Change value**.
    - **Decrement**: The risk index of the table column (target) is decreased by a fixed value. This value is specified in **Weighting/Change value**.
    - **Average (weighted)**: The average of all relevant risk indexes is calculated, weighted, and taken as basis for the next calculation.
    - **Average (normalized)**: The average of all relevant risk indexes is calculated with the normalized weighting factor and taken as basis for the next calculation.
    - **Reduction**: Used when calculating the reduced risk index for compliance rules, SAP functions, company policies, and attestation policies. You cannot add custom functions with this calculation type!
5. Use the slider next to **Weighting/change value** to set the value with which to weight the risk index in the overall calculation or by which value the risk index will be changed respectively.
6. (Optional) To disable the risk index function, select the check box next to **Disable**.
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1001
- Risk assessment (page description)

Enabling/disabling risk index functions

If you do not want to use a risk index function anymore, you can disable it. You can re-enable disabled risk index functions.

To disable a risk index function

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Runs**.
3. On the **Risk Assessment** page, in the list, click the risk index function that you want to disable.
4. In the dialog, check the **Disable** check box.
5. Click **Save**.

To enable a risk index function

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Attestation Policy Runs**.
3. On the **Risk Assessment** page, in the list, click the risk index function that you want to enable.
4. In the dialog, check the **Enable** check box.
5. Click **Save**.

Related topics

- Governance administration (page description) on page 1001
- Risk assessment (page description)

Displaying compliance frameworks

Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements.

To display compliance frameworks

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Compliance Frameworks**.

   This opens the **Compliance Frameworks** page (see Compliance frameworks (page description) on page 1004).
3. (Optional) To display more details of a compliance framework, click on the compliance framework in the list.

   This opens a new page with an overview of the framework with all its assigned rules, policies, and attestation policies (see Compliance framework details (page description) on page 1004).

Related topics

- Governance administration (page description) on page 1001
- Compliance frameworks (page description) on page 1004
- Compliance framework details (page description) on page 1004

Displaying high risk objects

You can display an overview of the objects with the highest risk factor in Web Portal. This can help you prioritize when managing your business resources. Company resources have risk values, which provide the risk index when combined with risk index functions.

To display the high risk object overview

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **High Risk Overview**.

   This opens the **High Risk Overview** page (see High risk overview (page description) on page 1005).
3. (Optional) Click a section header to display the corresponding objects.
4. (Optional) To display all high risk objects, select the check box next to **Show all high risk objects**.

Related topics

- Governance administration (page description) on page 1001
- High risk overview (page description) on page 1005

Displaying compliance rules and rule violations

You can see an overview of the compliance rules and corresponding rule violations in the Web Portal. This information can help to determine gaps in your security or compliance policies and to develop attestation policies or mitigating controls. Mitigating controls are processes existing outside the One Identity Manager solution and reduce the risk of violation.

To display an overview of compliance rules and rule violations

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Rule Violations**.

This opens the **Rule Violations** page (see Rule violations (page description) on page 1006).

3. Enable one of the options to specify how to display the compliance rules (see Rule violations (page description) on page 1006).
4. (Optional) To display more details about a compliance rules as a HyperView, perform the following:
    a. In the list, click the compliance rule whose details you want to show.
    b. In the details pane, click **Show details**.

    This opens a new page (see Rule details (page description) on page 1008).

Related topics

- Managing rule violations on page 201
- Governance administration (page description) on page 1001
- Rule violations (page description) on page 1006
- Rule details (page description) on page 1008

Displaying reports about compliance rules and rule violations

You can generate reports that describe the rule violations exactly. These reports contain a risk assessment for you to use for prioritizing violations and on which to base subsequent planning. The reduced risk index takes into account many risk factors that arise from violations and represents the risk as a value between 0 (no risk) and 1 (high risk).

To display a report about a compliance rule and its rule violations

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Rule Violations**.
3. On the **Rule Violations** page, enable one of the options to specify how to display the compliance rules (see Rule violations (page description) on page 1006).
4. In the list, click the compliance rule that you want to display a report about.
5. In the details pane, click **Report**.

Related topics

- Managing rule violations on page 201
- Governance administration (page description) on page 1001
- Rule violations (page description) on page 1006
- Rule details (page description) on page 1008

Displaying company policies and violations

You can see an overview of the company policies and corresponding policy violations in the Web Portal. This information can help to determine gaps in your security or compliance policies and to develop attestation policies or mitigating controls. Mitigating controls are processes existing outside the One Identity Manager solution and reduce the risk of violation.

To display an overview of company policies and policy violations

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Policy Violations**.

   This opens the **Policy Violations** page (see Policy violations (page description) on page 1009).
3. Enable one of the options to specify how to display the company policies (see Policy violations (page description) on page 1009).
4. (Optional) To display more details about a company policies as a HyperView, perform the following:
   a. In the list, click the company policy whose details you want to show.
   b. In the details pane, click **Show details**.

      This opens a new page (see Policy details (page description) on page 1010).

Related topics

- Managing policy violations on page 205
- Governance administration (page description) on page 1001
- Policy violations (page description) on page 1009
- Policy details (page description) on page 1010

Displaying reports about company policies and violations

You can generate reports that describe the policy violations exactly. These reports contain a risk assessment for you to use for prioritizing violations and on which to base subsequent planning. The reduced risk index takes into account many risk factors that arise from violations and represents the risk as a value between 0 (no risk) and 1 (high risk).

To display a report about a company policy and its policy violations

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Policy Violations**.

3. On the **Policy Violations** page, enable one of the options to specify how to display the company policies (see Policy violations (page description) on page 1009).
4. In the list, click the company policy that you want to display a report about.
5. In the details pane, click **Report**.

Related topics

- Managing policy violations on page 205
- Governance administration (page description) on page 1001
- Policy violations (page description) on page 1009
- Policy details (page description) on page 1010

Displaying compliance rules with SAP functions

Identities who have access to certain critical SAP functions, may violate compliance rules and can pose a significant security threat. You can analyze and determine these identities in order to prepare countermeasures.

By using the rule analysis, you can show the compliance rules that contain SAP functions and identify every identity that violates the rules. You can analyze the rule violation to determine the cause.

To display compliance rule with SAP functions

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Rule Violations**.

   This opens the **Rule Violations** page and shows a list with compliance rule containing SAP functions.
3. (Optional) To show whether user accounts and identities violate a compliance rule, in the list, click the compliance rule.
4. (Optional) You can determine whether the violation was caused by the role or instance in the case of each identity that has violated the rule. Perform one of the following actions:
   - To display details about rule violations of roles and profiles, click **By role** in the corresponding row.
   - To display details of SAP functions and transactions, click **By ability** in the corresponding row.

   This opens a new page (see Rule Analysis – Rule (page description) on page 1011).

Related topics

- Governance administration (page description) on page 1001
- Rule analysis (page description) on page 1011
- Rule Analysis – Rule (page description) on page 1011

Displaying rule violations of identities with critical SAP functions

Identities who have access to certain critical SAP functions, may violate compliance rules and can pose a significant security threat. You can analyze and determine these identities in order to prepare countermeasures.

Functional analysis allows you to display identities with critical SAP functions that violate compliance rules. For each identity, you can determine what SAP function is involved in the violation and the rules that caused the violation. If a rule with a significance rating is violated by an SAP function with a significance rating you must handle it promptly.

To display rule violations of identities with critical SAP functions

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **Critical Function Analysis**.

   This opens the **Rule violations by user** page and displays a list with identities that have critical SAP functions (see Rule violations by user (page description) on page 1012).
3. (Optional) To display an identity's SAP functions and rule violations, click the identity in the list.

   This opens a new page (see Rule violations for an identity (page description) on page 1013).

Related topics

- Displaying my identities' rule violations on page 302
- Governance administration (page description) on page 1001
- Rule violations by user (page description) on page 1012
- Rule violations for an identity (page description) on page 1013

6

Responsibilities

In One Identity Manager, identities have responsibilities for various objects. In the Web Portal, you can perform a number of actions on these responsibilities and obtain information about them.

Detailed information about this topic

- My responsibilities on page 218
- Delegating tasks on page 458
- Ownerships on page 463
- Auditing on page 466
- Governance administration on page 590

My responsibilities

You can manage objects that you are responsible for within your company. Possible objects are:

- Identities
- Devices
- Hierarchical roles
  - Organizations
    - Departments
    - Cost centers
    - Locations
  - Business roles
- Company resources
  - System roles
  - System entitlements

- System entitlements
- Application roles
- Resources
- Assignment resources
- Multi-request resources
- Multi requestable/unsubscribable resources
- Software

Detailed information about this topic

- Managing my identities on page 298
- Managing my system entitlements on page 407
- Managing my business roles on page 269
- Managing my system roles on page 430
- Managing my departments on page 220
- Managing my cost centers on page 318
- Managing my locations on page 383
- Managing my application roles on page 244
- Managing my resources on page 361
- Managing my assignment resources on page 450
- Managing my multi-request resources on page 342
- Managing my multi requestable/unsubscribable resources on page 350
- Managing my software applications on page 372
- Managing my devices on page 262

Specifying keywords for requestable products

You can assign tags for products that can be requested from the Web Portal. You define these tags in the associated service items of the corresponding objects.

Tags help requesters to quickly find the product they are looking for. You can run this search within the Web Portal.

For more information about tags, see the *One Identity Manager IT Shop Administration Guide*.

To specify a tag for a service item

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click the appropriate object type (for example, **System Entitlements**).
3. In this list, click the object for whose service item you want to specify a tag.
4. On the overview page, click **Main data**.
5. On the **Main data - <object name>** page, click on the name of the assigned service item in the **Service item** field.
6. On the overview page of the service item, click **Tags**.
7. (Optional) To create a new tag, perform the following actions on the **Tags** page:
    a. Click **New tag**.
    b. In the **Create a new tag** dialog, fill out the fields:
        - **Change label**: Enter the tag.
        - **Description**: Enter a description for the tag.
    c. Click **Save**.
8. On the **Tags** page, click (**Assign**) next to the tag that you want to set for the service item.

    This changes the icon in front of the tag ().

    TIP: Tags that are already assigned to the service item are marked with the icon.
9. Click **Save**.

Managing my departments

You can perform a variety of actions on the departments that you manage and gather information about them.

Detailed information about this topic

- Displaying my departments on page 221
- Restoring my deleted departments on page 221
- Displaying my department overviews on page 222
- Displaying and editing my department main data on page 223
- My department's memberships on page 223
- My department entitlements on page 225
- Compliance: My departments on page 228
- My departments' attestations on page 231
- Displaying my department risk indexes on page 236

- My departments' history on page 237
- Displaying role memberships of my department members on page 240
- Copying/splitting my departments on page 241
- Comparing and merging my departments on page 242
- Displaying my department statistics on page 244

Displaying my departments

You can see all the departments for which you are responsible.

To display departments

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.

   This opens the **Departments** page (see Departments (page description) on page 1076) and displays all the departments for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076

Restoring my deleted departments

You can restore deleted departments for which you were responsible. For example, a department can be deleted if two roles are merged during comparison (see Comparing and merging my departments on page 242).

To restore a deleted department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click **Restore a deleted role**.
4. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the department was deleted.
5. Next to the department you want to restore, select the check box.
6. Click **Next**.
7. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
8. Click **Next**.
9. Click **Close**.

To restore a deleted child department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department that was originally parent to the deleted department.
4. On the overview page, click **Restore**.
5. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the department was deleted.
6. In the list next to the department you want to restore, select the check box.
7. Click **Next**.
8. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
9. Click **Next**.
10. Click **Close**.

Related topics

- Comparing and merging my departments on page 242
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077

Displaying my department overviews

You can see all the relevant information about departments that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a department's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <department name>** page (see Overview – Department (page description) on page 1079).

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Overview – Department (page description) on page 1079

Displaying and editing my department main data

You can edit the main data of the departments for which you are responsible.

To display and edit a department's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Identities** page, click the department whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <department name>**, make your changes in the respective fields (see Main data – Department (page description) on page 1079).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Main data – Department (page description) on page 1079

My department's memberships

You can assign identities to departments for which you are responsible. You can see these identities, assign further identities to the departments and remove identities from the departments.

Detailed information about this topic

- Displaying memberships in my departments on page 224
- Assigning identities to my departments on page 224
- Removing identities from my departments on page 225

Displaying memberships in my departments

You can see identities that are assigned departments for which you are responsible.

To display identities that are assigned a department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <department name>** page (see Memberships – Department (page description) on page 1080).

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Memberships – Department (page description) on page 1080

Assigning identities to my departments

You can assign identities to departments for which you are responsible. You do this through requests.

To assign an identity to a department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department you want to assign an identity to.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <department name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the department.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   > TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the department.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Memberships – Department (page description) on page 1080
- My shopping cart (page description) on page 869

Removing identities from my departments

You can remove identities from departments for which you are responsible.

To remove an identity from a department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <department name>** page, select the check box next to the department that you want to remove.
6. Click **Delete memberships**.

   This cancels the department's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Memberships – Department (page description) on page 1080

My department entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to system roles you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the departments.

Detailed information about this topic

- Displaying my department entitlements on page 226
- Adding my department entitlements on page 226
- Deleting my department entitlements on page 227

Displaying my department entitlements

You can see entitlements that are assigned departments for which you are responsible. You can also display the reason why departments have certain entitlements (entitlement origin).

To display a department's entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <department name>** page (see Entitlements – Department (page description) on page 1081).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Entitlements – Department (page description) on page 1081

Adding my department entitlements

You can add entitlements to departments for which you are responsible. You do this through requests.

To assign an entitlement to a department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department to which you want to add an entitlement.
4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <department name>** page, click **Add new**.
6. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
7. Click **Assign**.
8. In the **Entitlement** dialog, in the list, click the entitlement that you want to add to the business role.
9. In the **Add a new entitlement** dialog, click **Request**.
10. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    After the request has been granted approval, the entitlement is added to the department.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Entitlements – Department (page description) on page 1081

Deleting my department entitlements

You can delete entitlements that are assigned departments for which you are responsible.

To delete an entitlement of a department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose entitlements you want to delete.
4. On the overview page, click **Entitlements**.

5. On the **Entitlements - <department name>** page, in the list, select the check box in the row of the entitlement you want to delete.
6. Click **Delete**.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Entitlements – Department (page description) on page 1081

Compliance: My departments

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying my departments' rule violations on page 229
- Displaying my department policy violations on page 229
- Displaying rule violations of my department members on page 230
- Displaying risk indexes and entitlements of my department members on page 230

Displaying my departments' rule violations

You can see the rule violations of departments for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose rule violations you want to display.
4. On the overview page, click **Compliance**.

   This opens the **Compliance - <department name>** page (see Compliance – Department (page description) on page 1082).

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Compliance – Department (page description) on page 1082

Displaying my department policy violations

You can see the policy violations of departments for which you are responsible.

To display policy violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose policy violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <department name>** page (see Compliance reports – Department (page description) on page 1088).
5. In the **View** menu, select **Policy violations**.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Compliance reports – Department (page description) on page 1088

Displaying rule violations of my department members

You can see the rule violations of identities that are assigned departments for which you are responsible.

To display rule violations of a department's members

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose rule violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <department name>** page (see Compliance reports – Department (page description) on page 1088).
5. In the **View** menu, select **Compliance rule violations**.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Compliance reports – Department (page description) on page 1088

Displaying risk indexes and entitlements of my department members

For every department that you are responsible for, you can see all the identities that have these department as primary or secondary assignments. You can also display the number of permissions assigned and the risk index.

To display members of a department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose members you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <department name>** page (see Compliance reports – Department (page description) on page 1088).
5. In the **View** menu, select **Identities: Risk indexes and entitlements**.
6. (Optional) To display more information about an identity, perform the following actions:

a. In the list, click an identity.
b. In the dialog, click **Overview**.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Compliance reports – Department (page description) on page 1088

My departments' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my department attestation cases on page 231
- Displaying attestors of my department pending attestation cases on page 233
- Approving and denying my department attestation cases on page 234
- Sending reminders about my department pending attestation cases on page 235

Displaying my department attestation cases

You can see attestation cases that involve departments for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <department name>** page (see Attestation – Department (page description) on page 1083).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Attestation – Department (page description) on page 1083

Displaying attestors of my department pending attestation cases

You can see identities that still have pending attestation cases from departments for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Attestation – Department (page description) on page 1083

Approving and denying my department attestation cases

You can grant or deny approval to attestation cases of departments for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
6. Click **Approve**.
7. On the **Attestation - <department name>** page, perform one of the following actions:
    - Click (**Approve**) next to the attestation case you want to approve.
    - Click (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Attestation – Department (page description) on page 1083

Sending reminders about my department pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the departments whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the departments whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the departments whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Attestation – Department (page description) on page 1083

Displaying my department risk indexes

You can see risk indexes of departments for which you are responsible.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a department's risk index

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose risk index you want to display.
4. On the overview page, click **Risk**.

   This opens the **Risk - <department name>** page (see Risk – Department (page description) on page 1085).
5. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Risk – Department (page description) on page 1085

My departments' history

The Web Portal gives you the option of displaying the historical data of departments for which you are responsible.

To do this, you have the following options:

Table 23: Historical data

View	Description
Events	This shows you all the events that affect the department, either on a timeline or in a table (see Displaying my department history on page 238).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my departments on page 239).
Status comparison	You can select a date and display all the changes made from then

View	Description
	until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my departments on page 239).

Displaying my department history

You can see all the events affecting departments that you are responsible for, either on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <department name>** page (see History – Department (page description) on page 1086).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.
5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- History – Department (page description) on page 1086

Displaying the status overview of my departments

You can see all the changes effecting departments for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <department name>** page (see History – Department (page description) on page 1086).
5. Click the **Status overview** tab.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- History – Department (page description) on page 1086

Comparing statuses of my departments

You can compare the current status of a department that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose status you want to compare.
4. On the overview page, click **History**.

5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since creation, deselect the check box next to **Display changed values only**.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- History – Department (page description) on page 1086

Displaying role memberships of my department members

You can display the roles and organizations belonging to identities that are assigned departments for which you are responsible. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose members you want to know more about.
4. On the overview page, click **Usage**.

This opens the **Usage - <department name>** page (see Usage – Department (page description) on page 1088).

5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click ⓘ (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Usage – Department (page description) on page 1088

Copying/splitting my departments

You can copy or move memberships and entitlements from departments you are responsible for to new roles (departments, business roles, cost centers, locations).

Any combination of role types is allowed.

To copy a department or move memberships and entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page click the department you want to copy or whose memberships and entitlements you want to move.
4. On the overview page, click **Split**.
5. In the **Split a role** dialog, in the **Type of the new role** menu, select a type for the new role.
6. Depending on which role type you have selected, enter the corresponding main data of the new role (see Main data – Department (page description) on page 1079, Main data – Business role (page description) on page 1050, Main data – Cost center (page description) on page 1093, or Main data - Location (page description) on page 1106).
7. Click **Next**.
8. Perform the following actions:
    - To neither copy nor move a entitlement/membership to a new role, click **Actions** > **Keep this assignment** next to the corresponding entitlement/membership. Later, the entitlement/membership is only available in the source role.

- To copy a entitlement/membership to a new role, click **Actions** > **Keep and copy to new role** next to the corresponding entitlement/membership. The entitlement/membership is later included in the source role as well as the target role.
- To move a entitlement/membership to a new role, click **Actions** > **Move to new role** next to the corresponding entitlement/membership. The entitlement/membership is later removed from the source role and is only included in the target role.

9. Click **Next**.
10. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.
12. Click **Close**.

Related topics

- My department's memberships on page 223
- My department entitlements on page 225
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077

Comparing and merging my departments

You can compare properties of departments that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a department

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department you want to compare and merge.
4. On the overview page, click **Compare and merge**.
5. In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your department.
6. Click **Assign**.
7. In the **Comparison role** dialog, select the business role/department/cost center/location to compare.

The assigned memberships and entitlements of both objects are listed with the following information:

Table 24: Overview of the assignments

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Object</td><td>Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.</td></tr>
<tr><td>Type</td><td>Type of the entitlement/membership.</td></tr>
<tr><td><Name of the source object></td><td rowspan="2">Shows you the entitlement/membership's assignment type. The following assignment types are available:
• Direct
• Inherited
• Requested
• Dynamic
• Not assigned
For more detailed information about assigning company resources, see the One Identity Manager Identity Management Base Module Administration Guide.</td></tr>
<tr><td><Name of the compare object></td></tr>
<tr><td>Comparison</td><td>Shows you where the entitlement/membership occurs.</td></tr>
</table>

> TIP: To arrange the list of assignments better, use the filters available some of the columns. For more information, see Filtering on page 40..

8. In the **Compare and merge** dialog, click **Merge the selected roles**.
9. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
10. Click **Next**.
11. Click **Close**.

Related topics

- My department's memberships on page 223
- My department entitlements on page 225
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077

Displaying my department statistics

You can see statistics of departments for which you are responsible. For example, you can see all the identities of a department that have not yet made a request.

To display a department's statistics

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Departments**.
3. On the **Departments** page, click the department whose statistics you want to display.
4. On the overview page, click **Statistics**.

   This opens the **Statistics for <department name>** dialog and shows the department's statistics.
5. (Optional) To obtain more information about a chart, click the chart or its header.

Related topics

- Discovering your statistics on the home page on page 795
- Statistics on page 795
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077

Managing my application roles

Use application roles to quickly and simply assign entitlement profiles to identities that match their tasks and functions. One Identity Manager already supplies a number of default application roles.

You can perform a variety of actions on the application roles that you manage and gather information about them.

Detailed information about this topic

- Displaying my application roles on page 245
- Displaying my application roles' overviews on page 245
- Creating your own application roles on page 246
- Displaying and editing my application roles' main data on page 246
- My application roles' memberships on page 247
- My application roles' reports on page 249
- Compliance: My application roles on page 250

- My application roles' attestations on page 252
- My application roles' history on page 258
- Displaying role memberships of my application roles' members on page 261

Displaying my application roles

You can see all the application roles for which you are responsible.

To display application roles

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.

   This opens the **Application Roles** page (see Application roles (page description) on page 1116) and displays all the application roles for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116

Displaying my application roles' overviews

You can see all the relevant information about application roles that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display an application role's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <application role name>** page (see Overview – Application role (page description) on page 1120).

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Overview – Application role (page description) on page 1120

Creating your own application roles

You can create new application roles for which you are responsible. You specify application role properties (for example memberships, entitlements and similar) later on.

To create a new application role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application roles** page, click **New application role**.
4. On the **Create a new application role** page, enter the application role's main data in the respective fields (see Creating new application roles (see (page description)) on page 1117).
5. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Creating new application roles (see (page description)) on page 1117

Displaying and editing my application roles' main data

You can edit the main data of the application roles that you are responsible for.

To display and edit an application role's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application roles whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <application role name>**, make your changes in the respective fields (see Main data - Application role (page description) on page 1120).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116

- Application role overview page (page description) on page 1118
- Main data - Application role (page description) on page 1120

My application roles' memberships

You can assign identities to application roles for which you are responsible. You can see these identities, assign further identities to the application roles and remove identities from the application roles.

Detailed information about this topic

- Displaying memberships in my application roles on page 247
- Assigning identities to my application roles on page 247
- Removing identities from my application roles on page 248

Displaying memberships in my application roles

You can see identities that are assigned application roles for which you are responsible.

To display identities that are assigned an application role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <application role name>** page (see Memberships – Application role (page description) on page 1121).

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Memberships – Application role (page description) on page 1121

Assigning identities to my application roles

You can assign identities to application roles for which you are responsible. You do this through requests.

To assign an identity to an application role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role you want to assign an identity to.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <application role name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the application role.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the application role.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Memberships – Application role (page description) on page 1121
- My shopping cart (page description) on page 869

Removing identities from my application roles

You can remove identities from application roles for which you are responsible.

To remove an identity from an application role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <application role name>** page, select the check box next to the application role that you want to remove.

6. Click **Delete memberships**.

   This cancels the application role's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Memberships – Application role (page description) on page 1121

My application roles' reports

Application roles can be assigned reports that are automatically subscribed to by all identities to which the respective application role has been assigned.

Detailed information about this topic

- Displaying my application roles' reports on page 249

Displaying my application roles' reports

You can see which reports are assigned to application roles for which you are responsible.

To display an application role's reports

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose assigned report you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <application role name>** page (see Entitlements – Application role (page description) on page 1122).

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Entitlements – Application role (page description) on page 1122

Compliance: My application roles

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying my application roles' policy violations on page 250
- Displaying rule violations of my application roles' members on page 251
- Displaying risk indexes and entitlements of my application roles' members on page 251

Displaying my application roles' policy violations

You can see the policy violations of application roles for which you are responsible.

To display policy violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose policy violations you want to display.
4. On the overview page, click **Compliance reports**.

This opens the **Compliance reports - <application role name>** page (see Compliance reports – Application role (page description) on page 1127).

5. In the **View** menu, select **Policy violations**.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Compliance reports – Application role (page description) on page 1127

Displaying rule violations of my application roles' members

You can see the rule violations of identities that are assigned application roles for which you are responsible.

To display rule violations of an application role's members

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose rule violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <application role name>** page (see Compliance reports – Application role (page description) on page 1127).
5. In the **View** menu, select **Compliance rule violations**.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Compliance reports – Application role (page description) on page 1127

Displaying risk indexes and entitlements of my application roles' members

For every application role that you are responsible for, you can see all the identities that have these application roles as primary or secondary assignments. You can also display the number of permissions assigned and the risk index.

To display members of an application role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose members you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <application role name>** page (see Compliance reports – Application role (page description) on page 1127).
5. In the **View** menu, select **Identities: Risk indexes and entitlements**.
6. (Optional) To display more information about an identity, perform the following actions:
   a. In the list, click an identity.
   b. In the dialog, click **Overview**.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Compliance reports – Application role (page description) on page 1127

My application roles' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my application roles' pending attestation cases on page 253
- Displaying attestors of my application roles' pending attestation cases on page 254
- Approving and denying my application roles' attestation cases on page 255
- Sending reminders about my application roles' pending attestation cases on page 256

Displaying my application roles' pending attestation cases

You can see attestation cases that involve application roles for which you are responsible. In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <application role name>** page (see Attestation – Application role (page description) on page 1123).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:

a. In the list, click the attestation case.

b. In the details pane, click the **History** tab.

This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Attestation – Application role (page description) on page 1123

Displaying attestors of my application roles' pending attestation cases

You can see identities that still have pending attestation cases from departments for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <application role name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

5. (Optional) On the **Attestations – <application role name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Attestation – Application role (page description) on page 1123

Approving and denying my application roles' attestation cases

You can grant or deny approval to attestation cases of application roles for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <application role name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Attestation - <application role>** page, perform one of the following actions:
   - Click (**Approve**) next to the attestation case you want to approve.
   - Click (**Deny**) next to the attestation case you want to deny.

   TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:

- For approved attestation case:
    - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
    - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
- For denied attestation cases:
    - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
    - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

> TIP: By giving reasons, your approvals are more transparent and support the audit trail.

> NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Attestation – Application role (page description) on page 1123

Sending reminders about my application roles' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application roles whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <application role name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application roles whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <application role name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application roles whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <application role name>** page, click on a tab to display the corresponding attestation cases.

6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Attestation – Application role (page description) on page 1123

My application roles' history

The Web Portal gives you the option of displaying the historical data of application roles for which you are responsible.

To do this, you have the following options:

Table 25: Historical data

View	Description
Events	This shows you all the events that affect the application role, either on a timeline or in a table (see Displaying my application roles' history on page 258).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my application roles on page 259).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my application roles on page 260).

Displaying my application roles' history

You can see all the events affecting application roles that you are responsible for, either on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <application role name>** page (see History – Application role (page description) on page 1125).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.
5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- History – Application role (page description) on page 1125

Displaying the status overview of my application roles

You can display all the changes effecting application roles for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <application role name>** page (see History – Application role (page description) on page 1125).
5. Click the **Status overview** tab.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- History – Application role (page description) on page 1125

Comparing statuses of my application roles

You can compare the current status of an application role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.

3. On the **Application Roles** page, click the application role whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since creation, deselect the check box next to **Display changed values only**.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- History – Application role (page description) on page 1125

Displaying role memberships of my application roles' members

You can display the roles and organizations belonging to identities that are assigned application roles for which you are responsible. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of an application role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Application roles**.
3. On the **Application Roles** page, click the application role whose members you want to know more about.
4. On the overview page, click **Usage**.

    This opens the **Usage - <application role name>** page (see Usage – Application role (page description) on page 1127).
5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- My responsibilities (page description) on page 1014
- Application roles (page description) on page 1116
- Application role overview page (page description) on page 1118
- Usage – Application role (page description) on page 1127

Managing my devices

You can perform a variety of actions on devices that you manage and gather information about them.

Detailed information about this topic

- Displaying my devices on page 262
- Adding your own devices on page 262
- Displaying my devices' overviews on page 263
- Displaying and editing my devices' main data on page 263

Displaying my devices

You can see all the devices for which you are responsible.

To display devices

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.

   This opens the **Devices** page (see Devices (page description) on page 1161) and displays all the devices for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Devices (page description) on page 1161

Adding your own devices

You can create new devices for which you are responsible.

To create a new device

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click **New device**.
4. On the **New device** page, enter the device's main data in the respective fields (see Adding new devices (page description) on page 1162).
5. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Devices (page description) on page 1161
- Adding new devices (page description) on page 1162

Displaying my devices' overviews

You can see all the relevant information about devices that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a device's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click the device whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <device name>** page (see Overview – Device (page description) on page 1165).

Related topics

- My responsibilities (page description) on page 1014
- Devices (page description) on page 1161
- Device overview page (page description) on page 1164
- Overview – Device (page description) on page 1165

Displaying and editing my devices' main data

You can edit the main data of the devices for which you are responsible.

To display and edit a device's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click the devices whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <device name>**, make your changes in the respective fields (see Main data – Device (page description) on page 1165).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Devices (page description) on page 1161
- Device overview page (page description) on page 1164
- Main data – Device (page description) on page 1165

My devices' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my devices' attestation cases on page 265
- Displaying attestors of my devices' pending attestation cases on page 266

- Approving and denying my devices' attestation cases on page 267
- Sending reminders about my devices' pending attestation cases on page 268

Displaying my devices' attestation cases

You can see attestation cases that involve devices for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <device name>** page (see).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014

- Devices (page description) on page 1161
- Device overview page (page description) on page 1164
- Attestations – Device (page description) on page 1168

Displaying attestors of my devices' pending attestation cases

You can see identities that still have pending attestation cases from devices for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <device name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <device name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Devices (page description) on page 1161

- Device overview page (page description) on page 1164
- Attestations – Device (page description) on page 1168

Approving and denying my devices' attestation cases

You can grant or deny approval to attestation cases of devices for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click the device whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <device name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Attestation - <device name>** page, perform one of the following actions:
    - Click ☑ (**Approve**) next to the attestation case you want to approve.
    - Click ☒ (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

10. Click **Save**.

Related topics

- Attestations
- My responsibilities (page description) on page 1014
- Devices (page description) on page 1161
- Device overview page (page description) on page 1164
- Attestations – Device (page description) on page 1168

Sending reminders about my devices' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <device name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <device name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Devices**.
3. On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <device name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Devices (page description) on page 1161
- Device overview page (page description) on page 1164
- Attestations – Device (page description) on page 1168

Managing my business roles

Business roles are defined based on resources to perform specific functions.

Business roles are objects for mapping company-specific functions in One Identity Manager. Business roles map company structures with similar functionality that exist in addition to departments, cost centers, and locations. This might be projects groups, for example.

You can carry out various actions on the system entitlements that you manage and obtain information about them.

Detailed information about this topic

- Displaying my business roles on page 270
- Creating your own business roles on page 271
- Restoring deleted my business roles on page 271
- Displaying my business roles' overviews on page 274
- Displaying and editing my business roles' main data on page 275
- My business roles' memberships on page 275
- My business roles' entitlements on page 277
- Compliance: My business roles on page 280
- My business roles' attestations on page 283
- Displaying my business roles' risk indexes on page 289
- My business roles' history on page 289
- Displaying role memberships of my business roles' members on page 294
- Copying/splitting my business roles on page 294
- Comparing and merging my business roles on page 296

Displaying my business roles

You can see all the business roles for which you are responsible.

To display business roles

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.

   This opens the **Business Roles** page (see Business roles (page description) on page 1046) and displays all the business roles for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046

Creating your own business roles

You can create new business roles for which you are responsible.

To create a new business role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business roles** page, click **New business role**.
4. On the **Create a new business role** page, enter the business role's main data in the respective fields (see Creating new business roles (page description) on page 1046).
5. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Creating new business roles (page description) on page 1046

Restoring deleted my business roles

You can restore deleted business roles for which you were responsible. For example, a business role can be deleted if two roles are merged during comparison (see Comparing and merging my business roles on page 296).

You can restore deleted departments for which you were responsible. For example, a department can be deleted if two roles are merged during comparison (see Comparing and merging my departments on page 242).

You can restore deleted cost centers for which you were responsible. For example, a cost center can be deleted if two roles are merged during comparison (see Comparing and merging my cost centers on page 340).

You can recover deleted locations for which you were responsible. For example, a location can be deleted if two roles are merged during comparison (see Comparing and merging my locations on page 405).

To restore a deleted business role

To restore a deleted department

To restore a deleted cost center

To restore a deleted location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.

   On the **My Responsibilities** page, click **Departments**.

   On the **My Responsibilities** page, click **Cost centers**.

   On the **My Responsibilities** page, click **Locations**.
3. On the **Business Roles** page, click **Restore a deleted role**.

   On the **Departments** page, click **Restore a deleted role**.

   On the **Cost Centers** page, click **Restore a deleted role**.

   On the **Locations** page, click **Restore a deleted role**.
4. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the business role was deleted.

   In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the department was deleted.

   In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the cost center was deleted.

   In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the location was deleted.
5. Next to the business role you want to restore, select the check box.

   Next to the department you want to restore, select the check box.

   Next to the cost center you want to restore, select the check box.

   Next to the location you want to restore, select the check box.
6. Click **Next**.
7. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
8. Click **Next**.
9. Click **Close**.

To restore a deleted child business role

To restore a deleted child department

To restore a deleted child cost center

To restore a deleted child location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.

   On the **My Responsibilities** page, click **Departments**.

   On the **My Responsibilities** page, click **Cost centers**.

   On the **My Responsibilities** page, click **Locations**.
3. On the **Business Roles** page, click the business role that was originally parent to the deleted business role.

   On the **Departments** page, click the department that was originally parent to the deleted department.

   On the **Cost Centers** page, click the cost center that was originally parent to the deleted cost center.

   On the **Locations** page, click the location that was originally parent to the deleted location.
4. On the overview page, click **Restore**.
5. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the business role was deleted.

   In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the department was deleted.

   In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the cost center was deleted.

   In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the location was deleted.
6. In the list next to the business role you want to restore, select the check box.

   In the list next to the department you want to restore, select the check box.

   In the list next to the cost center you want to restore, select the check box.

   In the list next to the location you want to restore, select the check box.
7. Click **Next**.
8. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
9. Click **Next**.
10. Click **Close**.

Related topics

- Comparing and merging my business roles on page 296
- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Comparing and merging my departments on page 242
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Comparing and merging my cost centers on page 340
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Comparing and merging my locations on page 405
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103

Displaying my business roles' overviews

You can see all the relevant information about business roles that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a business role's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <business role name>** page (see Overview – Business role (page description) on page 1050).

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046

- Business role overview page (page description) on page 1047
- Overview – Business role (page description) on page 1050

Displaying and editing my business roles' main data

You can edit the main data of the business roles for which you are responsible.

To display and edit a business role's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <business role name>**, make your changes in the respective fields (see Main data – Business role (page description) on page 1050).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Main data – Business role (page description) on page 1050

My business roles' memberships

You can assign identities to business roles for which you are responsible. You can see these identities, assign further identities to the business roles and remove identities from the business roles.

Detailed information about this topic

- Displaying my business roles' memberships on page 275
- Assigning identities to my business roles on page 276
- Removing identities from my business roles on page 277

Displaying my business roles' memberships

You can see identities that are assigned business roles for which you are responsible.

To display identities that are assigned a business role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <business role name>** page (see Memberships – Business role (page description) on page 1051).

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Memberships – Business role (page description) on page 1051

Assigning identities to my business roles

You can assign identities to business roles for which you are responsible. You do this through requests.

To assign an identity to a business role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business roles** page, click the business role you want to assign an identity to.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <business role name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the business role.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the business role.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Memberships – Business role (page description) on page 1051
- My shopping cart (page description) on page 869

Removing identities from my business roles

You can remove identities from business roles for which you are responsible.

To remove an identity from a business role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business roles** page, click the business role you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <business role name>** page, select the check box next to the business role that you want to remove.
6. Click **Delete memberships**.

   This cancels the business role's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Memberships – Business role (page description) on page 1051

My business roles' entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. Assigning identities to business roles avoids you having to assign entitlements separately to each identity. All a business role's entitlements are automatically assigned to all the identities assigned to the business role.

Detailed information about this topic

- Displaying my business roles' entitlements on page 278
- Adding my business roles' entitlements on page 278
- Deleting my business roles' entitlements on page 279

Displaying my business roles' entitlements

You can see entitlements that are assigned business roles for which you are responsible. You can also display the reason why business roles have certain entitlements (entitlement origin).

To display a business role's entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <business role name>** page (see Entitlements – Business role (page description) on page 1052).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Entitlements – Business role (page description) on page 1052

Adding my business roles' entitlements

You can add entitlements to business roles for which you are responsible. You do this through requests.

To assign an entitlement to a business role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role to which you want to add an entitlement.
4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <business role name>** page, click **Add new**.
6. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
7. Click **Assign**.
8. In the **Entitlement** dialog, in the list, click the entitlement that you want to add to the business role.
9. In the **Add a new entitlement** dialog, click **Request**.
10. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    After the request has been granted approval, the entitlement is added to the business role.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Entitlements – Business role (page description) on page 1052
- My shopping cart (page description) on page 869

Deleting my business roles' entitlements

You can delete entitlements that are assigned business roles for which you are responsible.

To delete an entitlement of a business role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose entitlements you want to delete.
4. On the overview page, click **Entitlements**.

5. On the **Entitlements - <business role name>** page, in the list, select the check box in the row of the entitlement you want to delete.
6. Click **Delete**.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Entitlements – Business role (page description) on page 1052

Compliance: My business roles

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying my business roles' rule violations on page 281
- Displaying my business roles' policy violations on page 281
- Displaying rule violations of my business roles' members on page 282
- Displaying risk indexes and entitlements of my business roles' members on page 282

Displaying my business roles' rule violations

You can see the rule violations of business roles for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose rule violations you want to display.
4. On the overview page, click **Compliance**.

   This opens the **Compliance - <business role name>** page (see Compliance – Business role (page description) on page 1053).

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Compliance – Business role (page description) on page 1053

Displaying my business roles' policy violations

You can see the policy violations of business roles for which you are responsible.

To display policy violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose policy violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <business role name>** page (see Compliance reports – Business role (page description) on page 1059).
5. In the **View** menu, select **Policy violations**.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Compliance reports – Business role (page description) on page 1059

Displaying rule violations of my business roles' members

You can see the rule violations of identities that are assigned business roles for which you are responsible.

To display rule violations of a business role's members

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose rule violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <business role name>** page (see Compliance reports – Business role (page description) on page 1059).
5. In the **View** menu, select **Compliance rule violations**.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Compliance reports – Business role (page description) on page 1059

Displaying risk indexes and entitlements of my business roles' members

For every business role that you are responsible for, you can see all the identities that have these business roles as primary or secondary assignments. You can also display the number of permissions assigned and the risk index.

To display members of a business role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose members you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <business role name>** page (see Compliance reports – Business role (page description) on page 1059).
5. In the **View** menu, select **Identities: Risk indexes and entitlements**.
6. (Optional) To display more information about an identity, perform the following actions:

a. In the list, click an identity.

b. In the dialog, click **Overview**.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Compliance reports – Business role (page description) on page 1059

My business roles' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my business roles' attestation cases on page 283
- Displaying attestors of my business roles' pending attestation cases on page 285
- Approving and denying my business roles' attestation cases on page 286
- Sending reminders about my business roles' pending attestation cases on page 287

Displaying my business roles' attestation cases

You can see attestation cases that involve business roles for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <business role name>** page (see Attestation – Business role (page description) on page 1054).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Attestation – Business role (page description) on page 1054

Displaying attestors of my business roles' pending attestation cases

You can see identities that still have pending attestation cases from business roles for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Attestation – Business role (page description) on page 1054

Approving and denying my business roles' attestation cases

You can grant or deny approval to attestation cases of business roles for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
6. Click **Approve**.
7. On the **Pending Attestations - <business role name>** page, perform one of the following actions:
   - Click (**Approve**) next to the attestation case you want to approve.
   - Click (**Deny**) next to the attestation case you want to deny.

   TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
   - For approved attestation case:
     - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
   - For denied attestation cases:
     - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
   - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

   TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Attestation – Business role (page description) on page 1054

Sending reminders about my business roles' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

This opens an email template with the attestor's email address.

10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Attestation – Business role (page description) on page 1054

Displaying my business roles' risk indexes

You can see risk indexes of business roles for which you are responsible.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a business role's risk index

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose risk index you want to display.
4. On the overview page, click **Risk**.

   This opens the **Risk - <business role name>** page (see Risk – Business role (page description) on page 1056).
5. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Risk – Business role (page description) on page 1056

My business roles' history

The Web Portal gives you the option of displaying the historical data of business roles for which you are responsible.

To do this, you have the following options:

Table 26: Historical data

View	Description
Events	This shows you all the events that affect the business role, either on a timeline or in a table (see Displaying my business roles' history on page 290).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only

View	Description
	see the initial and current status but you also see all the steps in between (see Displaying the status overview of my business roles on page 291).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my business roles on page 291).

Displaying my business roles' history

You can see all the events affecting business roles that you are responsible for, either on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <business role name>** page (see History – Business role (page description) on page 1057).

   TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

   To zoom in or out, turn the mouse wheel.
5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:

- Click on the event in the timeline.
- In the table view, click the event and you will see the details in the details pane.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- History – Business role (page description) on page 1057

Displaying the status overview of my business roles

You can see all the changes effecting business roles for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <business role name>** page (see History – Business role (page description) on page 1057).
5. Click the **Status overview** tab.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Overview – Business role (page description) on page 1050
- History – Business role (page description) on page 1057

Comparing statuses of my business roles

You can compare the current status of a business role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since creation, deselect the check box next to **Display changed values only**.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Overview – Business role (page description) on page 1050
- History – Business role (page description) on page 1057

Roll back my business roles to historical state

You can roll back a business role to a state in the past that is almost exactly like this state. In the process, you decide yourself which attributes to change. After selecting the business role, all attributes are displayed. These attributes can all be rolled back to a historical state, apart from a few exceptions.

In the following table, reasons are listed that prevent roll back to a historical state:

Table 27: Factors preventing rollback

Factor	Description
Attribute was not changed	Change is not possible without a comparative value.
Membership resulting from delegation	These memberships are not reset.
Inherited membership	These memberships cannot be deleted.
Membership resulting from a dynamic group	These memberships cannot be deleted.

To roll back a business role to a historical state

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role you want to roll back.
4. On the overview page, click **History**.
5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation, deselect the check box next to **Display changed values only**.
8. Select the check box next to the attribute that you want to roll back to a historical state.
9. Click **Roll back changes**.
10. (Optional) In the **Roll back changes** dialog box, check the actions that should be performed and, if necessary, clear the check boxes in front of the actions that should not be performed.
11. Click **Roll back**.

Related topics

My responsibilities (page description) on page 1014

Business roles (page description) on page 1046

Business role overview page (page description) on page 1047

History – Business role (page description) on page 1057

Displaying role memberships of my business roles' members

You can display the roles and organizations belonging to identities that are assigned business roles for which you are responsible. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a business role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose members you want to know more about.
4. On the overview page, click **Usage**.

   This opens the **Usage - <business role name>** page (see Usage – Business role (page description) on page 1059).
5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- Usage – Business role (page description) on page 1059

Copying/splitting my business roles

You can copy or move memberships and entitlements from business roles you are responsible for to new roles (departments, business roles, cost centers, locations).

Any combination of role types is allowed.

To copy a business role or move memberships and entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.

3. On the **Business Roles** page, click the business role you want to copy or whose memberships and entitlements you want to move.
4. On the overview page, click **Split**.
5. In the **Split a role** dialog, in the **Type of the new role** menu, select a type for the new role.
6. Depending on which role type you have selected, enter the corresponding main data of the new role (see Main data – Department (page description) on page 1079, Main data – Business role (page description) on page 1050, Main data – Cost center (page description) on page 1093, or Main data - Location (page description) on page 1106).
7. Click **Next**.
8. Perform the following actions:
    - To neither copy nor move a entitlement/membership to a new role, click **Actions** > **Keep this assignment** next to the corresponding entitlement/membership. Later, the entitlement/membership is only available in the source role.
    - To copy a entitlement/membership to a new role, click **Actions** > **Keep and copy to new role** next to the corresponding entitlement/membership. The entitlement/membership is later included in the source role as well as the target role.
    - To move a entitlement/membership to a new role, click **Actions** > **Move to new role** next to the corresponding entitlement/membership. The entitlement/membership is later removed from the source role and is only included in the target role.
9. Click **Next**.
10. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.
12. Click **Close**.

Related topics

- My business roles' memberships on page 275
- My business roles' entitlements on page 277
- Creating your own business roles on page 271
- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047

Comparing and merging my business roles

You can compare properties of business roles that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

You can compare properties of departments that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

You can compare properties of cost centers that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

You can compare properties of locations that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a business role

To compare and merge a department

To compare and merge a cost center

To compare and merge a location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Business Roles**.

   On the **My Responsibilities** page, click **Departments**.

   On the **My Responsibilities** page, click **Cost centers**.

   On the **My Responsibilities** page, click **Locations**.
3. On the **Business roles** page, click the business role that you want to compare and merge.

   On the **Departments** page, click the department you want to compare and merge.

   On the **Cost Centers** page, click the cost center you want to compare and merge.

   On the **Locations** page, click the location you want to compare and merge.
4. On the overview page, click **Compare and merge**.
5. In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your business role.

   In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your department.

   In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your cost center.

In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your location.

6. Click **Assign**.
7. In the **Comparison role** dialog, select the business role/department/cost center/location to compare.

   The assigned memberships and entitlements of both objects are listed with the following information:

Table 28: Overview of the assignments

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Object</td><td>Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.</td></tr>
<tr><td>Type</td><td>Type of the entitlement/membership.</td></tr>
<tr><td><Name of the source object></td><td rowspan="2">Shows you the entitlement/membership's assignment type. The following assignment types are available.
• Direct
• Inherited
• Requested
• Dynamic
• Not assigned
For more detailed information about assigning company resources, see the One Identity Manager Identity Management Base Module Administration Guide.</td></tr>
<tr><td><Name of the compare object></td></tr>
<tr><td>Comparison</td><td>Shows you where the entitlement/membership occurs.</td></tr>
</table>

TIP: To arrange the list of assignments better, use the filters available some of the columns. For more information, see Filtering on page 40..

8. In the **Compare and merge** dialog, click **Merge the selected roles**.
9. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
10. Click **Next**.
11. Click **Close**.

Related topics

- My business roles' memberships on page 275
- My business roles' entitlements on page 277
- Creating your own business roles on page 271

- My responsibilities (page description) on page 1014
- Business roles (page description) on page 1046
- Business role overview page (page description) on page 1047
- My department's memberships on page 223
- My department entitlements on page 225
- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- My cost center memberships on page 321
- My cost center entitlements on page 323
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- My locations' memberships on page 386
- My locations' entitlements on page 389
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103

Managing my identities

You can carry out various actions on the identities that you manage and obtain information about them.

Detailed information about this topic

- Assigning other managers to my identities on page 299
- Creating passcodes for my identities on page 300
- Displaying my identities on page 300
- Adding your own identities on page 301
- Displaying my identities' rule violations on page 302
- Displaying my identities' overviews on page 303
- Displaying and editing my identities' main data on page 301
- Creating reports about my identities on page 303
- Displaying my identity requests on page 304
- My identities' entitlements on page 304

- My identities' delegations on page 306
- My identities' attestations on page 308
- Displaying my identities' risk indexes on page 314
- My identities' history on page 315

Assigning other managers to my identities

You can assign other managers to the identities for which you are responsible.

To assign a new manager to an identity

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity that you want to assign to a new manager.
4. On the overview page, click **Main data**.
5. On the **Main data - <identity's name>**, click **Assign to new manager**.
6. On the **Assign New Manager** page, next to **New manager**, click **Assign**/**Change**.
7. In the **New manager** dialog box, click the manager you want to assign to the identity.
8. On the **Assign to new manager** page, in the **Effective date** field, set a date and time from which the new manager takes effect.
9. (Optional) If the identity for which you are selecting a new manager already has entitlements or products assigned, they are removed or unsubscribed by default on the effective date. If you want the identity to retain these entitlements or products when transferring to the new manager, disable the check boxes next to the respective entitlements and products.
10. Click **Submit**.
11. In the dialog, confirm the prompt with **Yes**.

    NOTE: On the **Pending Requests** page, your request to change managers is presented to the new manager to be granted or denied approval (see Approving new managers' pending requests on page 117). After the new manager approves this requests, the new manager is assigned.

Related topics

- Approving new managers' pending requests on page 117
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Main data – Identity (page description) on page 1020
- Assigning to new manager (page description) on page 1022

Creating passcodes for my identities

If identities, for which you are responsible, have forgotten their password for logging into the Web Portal and the passwords cannot be reset with the question and answer feature, you can create passcodes for them. With this passcode, identities can log on to the Password Reset Portal once and for a limited time.

To create a passcode for an identity

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity for which you want to create the passcode.
4. On the overview page, click **Passcode**.

   The generated passcode, its validity period, and a URL that the identity uses to login in to thePassword Reset Portal, are displayed in a dialog.
5. Note or copy the code and have it sent to the identity with the validity period.

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018

Displaying my identities

You can see all the identities for which you are responsible.

To display identities

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.

   This opens the **Identities** page (see Identities (page description) on page 1015) and displays all the identities that report directly to you.
3. (Optional) To show identities that report indirectly to you,deselect the **Show only direct reports** box.

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015

Displaying and editing my identities' main data

You can edit the main data of the identities for which you are responsible.

To display and edit an identity's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <identity name>**, make your changes in the respective fields (see Main data – Identity (page description) on page 1020).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Main data – Identity (page description) on page 1020

Adding your own identities

You can add new identities for which you are responsible. This function is mainly designed for adding external identities. For example, subcontractors who are not entered in the human resources department. Data from new identities is either transferred completely to the database or existing data is updated and/or augmented. This depends on the system configuration and the import setting from closed systems.

To add a new identity

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click **Add a new identity**.
4. On the **Add a new identity** page, enter the identity's main data in the respective fields (see Adding a new identity (page description) on page 1017).
5. Click **Save**.

   When saving, the system checks whether the combination of first and last name already exists.
6. Depending on the result of checking the name combination, perform one of the following actions:

- If this combination of names does not yet exist, confirm the prompt with **Yes**.
- If this combination of names already exists and you want to edit/update the existing identity:
    1. On the **Other identities with similar properties** page, in the list, click the identity that you want to edit/update.
    2. Click **Update identity data**.
    3. Confirm the prompt with **Yes** in the dialog.

       This edits/updates the identity data.
- If identical combinations already exists and you still want add a new identity:
    1. On the **Other identities with similar properties** page, click **Add a new identity**.
    2. Confirm the prompt with **Yes** in the dialog.

       This adds new identity data.

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Adding a new identity (page description) on page 1017

Displaying my identities' rule violations

You can display the rule violations of identities for which you are responsible.

To display identities' rule violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click **Rule violations**.

   This opens the **Rule violations by direct reports** page (see Rule violations of directly subordinated identities (page description) on page 1016).

Related topics

- Managing rule violations on page 201
- Displaying compliance rules and rule violations on page 213
- Displaying rule violations of identities with critical SAP functions on page 217
- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Rule violations of directly subordinated identities (page description) on page 1016

Displaying my identities' overviews

You can see all the relevant information about identities that report directly to you in the summarized form of an overview. For example, this information includes identities, requests, rule violations, user accounts, subidentities, assigned permissions, and memberships. The information is represented by shapes in a HyperView.

To display an identity's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <identity name>** page (see Overview – Identity (page description) on page 1020).

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Overview – Identity (page description) on page 1020

Creating reports about my identities

You can use the data from identities to create reports about those for which you are responsible.

To create a report about an identity

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity for which you want to create a report.
4. On the overview page, click **Main data**.
5. On the **Main data - <identity's name>**, click **Generate report**.
6. In the dialog, select one or both of the check boxes.
   - **Generate report including history**: A history with all changes to the identity is attached to the report.
   - **Include data for sub identities in the report**: The report additionally includes data for all the identity's sub identities.
7. Click **Generate report**.

Related topics

- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Main data – Identity (page description) on page 1020

Displaying my identity requests

You can display requests of identities for which you are responsible. All requests that identities have made themselves or that have been made for them (for example, by a manager) are displayed.

To display requests of an identity

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose requests you want to display.
4. On the overview page, click **Requests**.

   This opens the**Requests- <name of identity>** page (see Requests - Identity ((page description)) on page 1023).
5. (Optional) Click **Advanced Search** to control which requests are displayed (see Requests - Identity ((page description)) on page 1023). For example, you can display only pending (not yet assigned) requests.

Related topics

- Displaying request history on page 128
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Requests - Identity ((page description)) on page 1023

My identities' entitlements

Identities under the scope of your responsibility can own different entitlements. You can see these entitlements and delete them.

Detailed information about this topic

- Displaying my identities' entitlements on page 305
- Deleting my identities' entitlements on page 305

Displaying my identities' entitlements

You can see entitlements that are assigned identities for which you are responsible. You can also display the reason why identities have certain entitlements (entitlement origin).

To display an identity's entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <identity's name>** page (see Entitlements – Identity (page description) on page 1025).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Entitlements – Identity (page description) on page 1025

Deleting my identities' entitlements

You can delete entitlements that are assigned identities for which you are responsible.

To delete an entitlement of an identity

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose delegation you want to delete.
4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <identity>** page, in the list, select the check box in the row of the entitlement you want to delete.
6. Click **Delete memberships**.

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Entitlements – Identity (page description) on page 1025

My identities' delegations

Responsibilities or roles of identities that you manage, can be temporarily delegated to other identities. For example, the responsibility for a department can be given to another identity.

Detailed information about this topic

- Deleting my identities' delegations on page 306
- Adding delegations for my identities on page 307
- Canceling my identities' delegations on page 307
- Deleting my identities' delegations on page 308

Deleting my identities' delegations

You can see the delegations of identities for which you are responsible.

To display delegations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose delegations you want to display.
4. On the overview page, click **Delegations**.

   This opens the **Delegations - <identity name>** page (see Delegations – Identity (page description) on page 1026).

- Displaying delegations on page 458
- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Delegations – Identity (page description) on page 1026

Adding delegations for my identities

You can delegate role memberships and responsibilities of identities for which you are responsible to other identities. For example, you can give one identity's responsibility for a department to another identity.

NOTE: You cannot edit a delegation afterward. If you want to make a change to the delegation, delete the it and create a new delegation.

To create a delegation

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity who should become the delegate.
4. On the overview page, click **Delegations**.
5. On the **Delegations - <identity's name>**, click **New delegation**.
6. Click **Next**.
7. In the step, in the list, select the check boxes in front of the role memberships/responsibilities you want to delegate.
8. Click **Next**.
9. In the **Add additional information** set, configure the following settings:
    - **Valid from**: Specify from when the role/responsibility will be delegated.
    - **Valid until**: Specify until when the role/responsibility will be delegated.
    - **Notify me if the recipient of the delegation makes a decision**: (Optional) Select the check box if you want to be notified when the recipient makes an approval decision about a delegated role/responsibility.
    - **The recipient can delegate this role**: (Optional) Select the check box to specify that the recipient can delegate their delegated role/responsibility on to another identity.
    - **Reason**: (Optional) In the dialog, enter a reason for the delegation.
    - **Priority**: (Optional) In the menu, select a priority for the delegation.
10. Click **Save**.

- Creating delegations on page 459
- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Delegations – Identity (page description) on page 1026

Canceling my identities' delegations

You can cancel delegations of identities for which you are responsible.

NOTE: You can only cancel delegations as long they have the **Request** or **Approved** status. You can delete delegations with the **Assigned** status .

To cancel a delegation

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose delegation you want to cancel.
4. On the overview page, click **Delegations**.

- Canceling delegations on page 460
- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Delegations – Identity (page description) on page 1026

Deleting my identities' delegations

You can delete delegations of identities for which you are responsible.

NOTE: You can only delete delegations as long as they have the **Assigned** status. You can cancel delegations that have the **Request** or **Approved** status (see Canceling my identities' delegations on page 307).

To delete a delegation

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose delegation you want to delete.
4. On the overview page, click **Delegations**.

- Deleting delegations on page 461
- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Delegations – Identity (page description) on page 1026

My identities' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to

describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying attestors of my attestation cases on page 163
- Displaying attestation cases of my identities on page 309
- Approving and denying my identities' attestation cases on page 311
- Displaying attestors of my identities' pending attestation cases on page 310
- Sending reminders about my identities' pending attestation cases on page 312

Displaying attestation cases of my identities

You can see attestation cases that involve identities for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <identity's name>** page (see Attestations – Identity (page description) on page 1027).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.

c. In the **Attested object** dialog, select an object in the **Object** menu.

   This shows information about the object.

d. (Optional) Click **View current state of the object**

   This opens an overview in shapes of the attestation.

7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:

   a. In the list, click the attestation case.

   b. In the details pane, click the **Workflow** tab.

8. (Optional) To show previous attestation cases for the selected object, perform the following actions:

   a. In the list, click the attestation case.

   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Attestations – Identity (page description) on page 1027

Displaying attestors of my identities' pending attestation cases

You can see identities that still have pending attestation cases from identities for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Attestations – Identity (page description) on page 1027

Approving and denying my identities' attestation cases

You can grant or deny approval to attestation cases of identities for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.

7. On the **Pending attestations - <identity name>** page, perform one of the following actions:

    - Click ☑ (**Approve**) next to the attestation case you want to approve.
    - Click ☒ (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).

8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:

    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Attestations – Identity (page description) on page 1027

Sending reminders about my identities' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.

3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Attestations – Identity (page description) on page 1027

Displaying my identities' risk indexes

You can see risk indexes of identities for which you are responsible.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display an identity's risk index

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose risk index you want to display.
4. On the overview page, click **Risk**.

   This opens the **Risk - <identity's name>** page (see Risk – Identity (page description) on page 1029).
5. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- My responsibilities (page description) on page 1014

- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- Risk – Identity (page description) on page 1029

My identities' history

The Web Portal gives you the option of displaying the historical data of identities for which you are responsible.

To do this, you have the following options:

Table 29: Historical data

View	Description
Events	This shows you all the events that affect the identity, either on a timeline or in a table (see Displaying my identity history on page 315).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my identities on page 316).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my identities on page 317).

Displaying my identity history

You can see all the events affecting identities that you are responsible for, either on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <identity name>** page (see History – Identity (page description) on page 1030).

TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

To zoom in or out, turn the mouse wheel.

5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- History – Identity (page description) on page 1030

Displaying the status overview of my identities

You can see all the changes effecting identities for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose status overview you want to display.
4. On the overview page, click **History**.

This opens the **History - <identity's name>** page (see History – Identity (page description) on page 1030).

5. Click the **Status overview** tab.

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- History – Identity (page description) on page 1030

Comparing statuses of my identities

You can compare the current status of an identity that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Identities**.
3. On the **Identities** page, click the identity whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since creation, deselect the check box next to **Display changed values only**.

Related topics

- My responsibilities (page description) on page 1014
- Identities (page description) on page 1015
- Identity overview page (page description) on page 1018
- History – Identity (page description) on page 1030

Managing my cost centers

You can perform a variety of actions on cost centers that you manage and gather information about them.

Detailed information about this topic

- Displaying my cost centers on page 318
- Restoring my deleted cost centers on page 319
- Displaying my cost center overviews on page 320
- Displaying and editing my cost center main data on page 320
- My cost center memberships on page 321
- My cost center entitlements on page 323
- My cost centers' attestations on page 325
- Compliance: My cost centers on page 331
- Displaying my cost center risk indexes on page 334
- My cost center history on page 335
- Displaying role memberships of my cost center members on page 338
- Copying/splitting my cost centers on page 339
- Comparing and merging my cost centers on page 340
- Displaying my cost center statistics on page 341

Displaying my cost centers

You can see all the cost centers for which you are responsible.

To display cost centers

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.

   This opens the **Cost Centers** page (see Cost centers (page description) on page 1090) and displays all the cost centers for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090

Restoring my deleted cost centers

You can restore deleted cost centers for which you were responsible. For example, a cost center can be deleted if two roles are merged during comparison (see Comparing and merging my cost centers on page 340).

To restore a deleted cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click **Restore a deleted role**.
4. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the cost center was deleted.
5. Next to the cost center you want to restore, select the check box.
6. Click **Next**.
7. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
8. Click **Next**.
9. Click **Close**.

To restore a deleted child cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center that was originally parent to the deleted cost center.
4. On the overview page, click **Restore**.
5. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the cost center was deleted.
6. In the list next to the cost center you want to restore, select the check box.
7. Click **Next**.
8. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
9. Click **Next**.
10. Click **Close**.

Related topics

- Comparing and merging my cost centers on page 340
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091

Displaying my cost center overviews

You can see all the relevant information about cost centers that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a cost center's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <cost center name>** page (see Overview – Cost center (page description) on page 1093).

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Overview – Cost center (page description) on page 1093

Displaying and editing my cost center main data

You can edit the main data of the cost centers for which you are responsible.

To display and edit a cost center's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost centers whose main data you want to display/edit.
4. On the overview page, click **Main data**.

5. On the **Main data - <cost center>**, make your changes in the respective fields (see Main data – Cost center (page description) on page 1093).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Main data – Cost center (page description) on page 1093

My cost center memberships

You can assign identities to cost centers for which you are responsible. You can see these identities, assign further identities to the cost centers and remove identities from the cost centers.

Detailed information about this topic

- Displaying memberships in my cost centers on page 321
- Assigning my identities to cost centers on page 322
- Removing identities from my cost centers on page 322

Displaying memberships in my cost centers

You can see identities that are assigned cost centers for which you are responsible.

To display identities that are assigned a cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <cost center name>** page (see Memberships – Cost center (page description) on page 1094).

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090

- Cost center overview page (page description) on page 1091
- Memberships – Cost center (page description) on page 1094

Assigning my identities to cost centers

You can assign identities to cost centers for which you are responsible. You do this through requests.

To assign an identity to a cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center you want to assign an identity to.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <cost center name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the cost center.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the cost center.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Memberships – Cost center (page description) on page 1094
- My shopping cart (page description) on page 869

Removing identities from my cost centers

You can remove identities from cost centers for which you are responsible.

To remove an identity from a cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.

3. On the **Cost Centers** page, click the cost center you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <cost center name>** page, select the check box next to the cost center that you want to remove.
6. Click **Delete memberships**.

   This cancels the cost center's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Memberships – Cost center (page description) on page 1094

My cost center entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to a cost center you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the cost center.

Detailed information about this topic

- Displaying my cost center entitlements on page 323
- Adding my cost center entitlements on page 324
- Deleting my cost center entitlements on page 325

Displaying my cost center entitlements

You can see entitlements that are assigned cost centers for which you are responsible. You can also display the reason why cost centers have certain entitlements (entitlement origin).

To display a cost center's entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

This opens the **Entitlements - <cost center name>** page (see Entitlements – Cost center (page description) on page 1095).

5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Entitlements – Cost center (page description) on page 1095

Adding my cost center entitlements

You can add entitlements to cost centers for which you are responsible. You do this through requests.

To assign an entitlement to a cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center to which you want to add an entitlement.
4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <cost center name>** page, click **Add new**.
6. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
7. Click **Assign**.
8. In the **Entitlement** dialog, in the list, click the entitlement that you want to add to the business role.
9. In the **Add a new entitlement** dialog, click **Request**.
10. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    After the request has been granted approval, the entitlement is added to the cost center.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Entitlements – Cost center (page description) on page 1095

Deleting my cost center entitlements

You can delete entitlements that are assigned cost centers for which you are responsible.

To delete an entitlement of a cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose entitlements you want to delete.
4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <cost center name>** page, in the list, select the check box in the row of the entitlement you want to delete.
6. Click **Delete**.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Entitlements – Cost center (page description) on page 1095

My cost centers' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my cost center attestation cases on page 326
- Displaying attestors of my cost center pending attestation cases on page 327
- Approving and denying my cost center attestation cases on page 328
- Sending reminders about my cost centers' pending attestation cases on page 329

Displaying my cost center attestation cases

You can see attestation cases that involve cost centers for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <cost center name>** page (see Attestation – Cost center (page description) on page 1097).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:

a. In the list, click the attestation case.

b. In the details pane, click the **Workflow** tab.

8. (Optional) To show previous attestation cases for the selected object, perform the following actions:

    a. In the list, click the attestation case.

    b. In the details pane, click the **History** tab.

    This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Attestation – Cost center (page description) on page 1097

Displaying attestors of my cost center pending attestation cases

You can see identities that still have pending attestation cases from cost centers for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

    The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.

3. On the **Cost Centers** page, click the cost center whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Attestation – Cost center (page description) on page 1097

Approving and denying my cost center attestation cases

You can grant or deny approval to attestation cases of cost centers for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Attestation - <cost center name>** page, perform one of the following actions:
   - Click ☑ (**Approve**) next to the attestation case you want to approve.
   - Click ☒ (**Deny**) next to the attestation case you want to deny.

   TIP: To grant or deny approval for all the attestation cases displayed, click ☑ (**Approve all**) or ☒ (**Deny all**).
8. Click **Next**.

9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
   - For approved attestation case:
     - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
   - For denied attestation cases:
     - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
   - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

   TIP: By giving reasons, your approvals are more transparent and support the audit trail.

   NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Attestation – Cost center (page description) on page 1097

Sending reminders about my cost centers' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).

- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost centers whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost centers whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost centers whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

5. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Attestation – Cost center (page description) on page 1097

Compliance: My cost centers

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying my cost center rule violations on page 332
- Displaying my cost center policy violations on page 332
- Displaying rule violations of my cost center members on page 333
- Displaying risk indexes and entitlements of my cost center members on page 333

Displaying my cost center rule violations

You can see the rule violations of cost centers for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose rule violations you want to display.
4. On the overview page, click **Compliance**.

   This opens the **Compliance - <cost center name>** page (see Compliance – Cost center (page description) on page 1096).

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Compliance – Cost center (page description) on page 1096

Displaying my cost center policy violations

You can see the policy violations of cost centers for which you are responsible.

To display policy violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose policy violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <cost center name>** page (see Compliance reports – Cost center (page description) on page 1102).
5. In the **View** menu, select **Policy violations**.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Compliance reports – Cost center (page description) on page 1102

Displaying rule violations of my cost center members

You can see the rule violations of identities that are assigned cost centers for which you are responsible.

To display rule violations of a cost center's members

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose rule violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <cost center name>** page (see Compliance reports – Cost center (page description) on page 1102).
5. In the **View** menu, select **Compliance rule violations**.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Compliance reports – Cost center (page description) on page 1102

Displaying risk indexes and entitlements of my cost center members

For every cost center that you are responsible for, you can see all the identities that have these cost center as primary or secondary assignments. You can also display the number of permissions assigned and the risk index.

To display members of a cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.

3. On the **Cost Centers** page, click the cost center whose members you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <cost center name>** page (see Compliance reports – Cost center (page description) on page 1102).
5. In the **View** menu, select **Identities: Risk indexes and entitlements**.
6. (Optional) To display more information about an identity, perform the following actions:
   a. In the list, click an identity.
   b. In the dialog, click **Overview**.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Compliance reports – Cost center (page description) on page 1102

Displaying my cost center risk indexes

You can see risk indexes of cost centers for which you are responsible.

> NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a cost center's risk index

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose risk index you want to display.
4. On the overview page, click **Risk**.

   This opens the **Risk - <cost center name>** page (see Risk – Cost center (page description) on page 1099).
5. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090

- Cost center overview page (page description) on page 1091
- Risk – Cost center (page description) on page 1099

My cost center history

The Web Portal gives you the option of displaying the historical data of cost centers for which you are responsible.

To do this, you have the following options:

Table 30: Historical data

View	Description
Events	This shows you all the events that affect the cost center, either on a timeline or in a table (see Displaying my cost center history on page 335).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my cost centers on page 336).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my cost centers on page 337).

Displaying my cost center history

You can see all the events affecting cost centers that you are responsible for, either on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <cost center name>** page (see History – Cost center (page description) on page 1100).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

To zoom in or out, turn the mouse wheel.

5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- History – Cost center (page description) on page 1100

Displaying the status overview of my cost centers

You can see all the changes effecting cost centers for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <cost center name>** page (see History – Cost center (page description) on page 1100).

5. Click the **Status overview** tab.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- History – Cost center (page description) on page 1100

Comparing statuses of my cost centers

You can compare the current status of a cost center that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since creation, deselect the check box next to **Display changed values only**.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- History – Cost center (page description) on page 1100

Displaying role memberships of my cost center members

You can display the roles and organizations belonging to identities that are assigned cost centers for which you are responsible. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose members you want to know more about.
4. On the overview page, click **Usage**.

   This opens the **Usage - <cost center name>** page (see Usage – Cost center (page description) on page 1102).
5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091
- Usage – Cost center (page description) on page 1102

Copying/splitting my cost centers

You can copy or move memberships and entitlements from cost centers you are responsible for to new roles (departments, business roles, cost centers, locations).

Any combination of role types is allowed.

To copy a cost center or move memberships and entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center you want to copy or whose memberships and entitlements you want to move.
4. On the overview page, click **Split**.
5. In the **Split a role** dialog, in the **Type of the new role** menu, select a type for the new role.
6. Depending on which role type you have selected, enter the corresponding main data of the new role (see Main data – Department (page description) on page 1079, Main data – Business role (page description) on page 1050, Main data – Cost center (page description) on page 1093, or Main data - Location (page description) on page 1106).
7. Click **Next**.
8. Perform the following actions:
    - To neither copy nor move a entitlement/membership to a new role, click **Actions** > **Keep this assignment** next to the corresponding entitlement/membership. Later, the entitlement/membership is only available in the source role.
    - To copy a entitlement/membership to a new role, click **Actions** > **Keep and copy to new role** next to the corresponding entitlement/membership. The entitlement/membership is later included in the source role as well as the target role.
    - To move a entitlement/membership to a new role, click **Actions** > **Move to new role** next to the corresponding entitlement/membership. The entitlement/membership is later removed from the source role and is only included in the target role.
9. Click **Next**.
10. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.
12. Click **Close**.

Related topics

- My cost center memberships on page 321
- My cost center entitlements on page 323
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091

Comparing and merging my cost centers

You can compare properties of cost centers that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a cost center

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center you want to compare and merge.
4. On the overview page, click **Compare and merge**.
5. In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your cost center.
6. Click **Assign**.
7. In the **Comparison role** dialog, select the business role/department/cost center/location to compare.

   The assigned memberships and entitlements of both objects are listed with the following information:

   Table 31: Overview of the assignments

Column	Description
Object	Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.
Type	Type of the entitlement/membership.
<Name of the source object>	Shows you the entitlement/membership's assignment type. The following assignment types are available. • Direct • Inherited

Column	Description
	• Requested • Dynamic
<Name of the compare object>	• Not assigned For more detailed information about assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.
Comparison	Shows you where the entitlement/membership occurs.

TIP: To arrange the list of assignments better, use the filters available some of the columns. For more information, see Filtering on page 40..

8. In the **Compare and merge** dialog, click **Merge the selected roles**.
9. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
10. Click **Next**.
11. Click **Close**.

Related topics

- My cost center memberships on page 321
- My cost center entitlements on page 323
- My responsibilities (page description) on page 1014
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091

Displaying my cost center statistics

You can see statistics of cost centers for which you are responsible.

To display a cost center's statistics

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose statistics you want to display.
4. On the overview page, click **Statistics**.

   This opens the **Statistics for <cost center name>** dialog and shows the cost center's statistics.
5. (Optional) To obtain more information about a chart, click the chart or its header.

Related topics

- Discovering your statistics on the home page on page 795
- Statistics on page 795
- Cost centers (page description) on page 1090
- Cost center overview page (page description) on page 1091

Managing my multi-request resources

The One Identity Manager distinguishes between single or multiple requestable products. Single request products are, for example, software, system roles, or Active Directory groups. These products cannot be requested if they have already been be requested for the same time period.

Furthermore, an identity may need several of one type of company resources, for example, consumables like pens or printer paper. You can find company resources such as these mapped in One Identity Manager as Multi-request resource or Multi requestable/unsubscribable resources.

Multi-request resources are automatically unsubscribed after the request is granted approval. The resources are not explicitly assigned to identities.

You can perform a variety of actions on the multi-request resources that you manage and gather information about them.

Detailed information about this topic

- Displaying my multi-request resources on page 342
- Displaying my multi-request resources' overviews on page 343
- Displaying and editing my multi-request resources' main data on page 343
- My multi-request resources' attestations on page 344

Displaying my multi-request resources

You can see all the multi-request resources for which you are responsible.

To display multi-request resources

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.

   This opens the **Multi-request Resources** page (see Multi-request resources (page description) on page 1141) and displays all the multi-request resources for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Multi-request resources (page description) on page 1141

Displaying my multi-request resources' overviews

You can see all the relevant information about multi-request resources that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a multi-request resource's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <multi-request resource name>** page (see Overview – Multi-request resource (page description) on page 1142).

Related topics

- My responsibilities (page description) on page 1014
- Multi-request resources (page description) on page 1141
- Multi-request resource overview page (page description) on page 1142
- Overview – Multi-request resource (page description) on page 1142

Displaying and editing my multi-request resources' main data

You can edit the main data of the multi-request resources for which you are responsible.

To display and edit a multi-request resource's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose main data you want to display/edit.
4. On the overview page, click **Main data**.

5. On the **Main data - <multi-request resource name>**, make your changes in the respective fields (see Main data – Multi-request resource (page description) on page 1143).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Multi-request resources (page description) on page 1141
- Multi-request resource overview page (page description) on page 1142
- Main data – Multi-request resource (page description) on page 1143

My multi-request resources' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my multi-request resources' attestation cases on page 345
- Displaying attestors of my multi-request resources' pending attestation cases on page 346
- Approving and denying my multi-request resources' attestation cases on page 347
- Sending reminders about my multi-request resources' pending attestation cases on page 348

Displaying my multi-request resources' attestation cases

You can see attestation cases that involve multi-request resources for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <multi-request resource name>** page (see Attestation – Multi-request resource (page description) on page 1144).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Multi-request resources (page description) on page 1141

- Multi-request resource overview page (page description) on page 1142
- Attestation – Multi-request resource (page description) on page 1144

Displaying attestors of my multi-request resources' pending attestation cases

You can see identities that still have pending attestation cases from multi-request resources for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Multi-request resources (page description) on page 1141

- Multi-request resource overview page (page description) on page 1142
- Attestation – Multi-request resource (page description) on page 1144

Approving and denying my multi-request resources' attestation cases

You can grant or deny approval to attestation cases of multi-request resources for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Attestation - <multi-request resource name>** page, perform one of the following actions:
    - Click ☑ (**Approve**) next to the attestation case you want to approve.
    - Click ☒ (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.

- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Multi-request resources (page description) on page 1141
- Multi-request resource overview page (page description) on page 1142
- Attestation – Multi-request resource (page description) on page 1144

Sending reminders about my multi-request resources' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.

8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Multi-request resources (page description) on page 1141
- Multi-request resource overview page (page description) on page 1142
- Attestation – Multi-request resource (page description) on page 1144

Managing my multi requestable/unsubscribable resources

The One Identity Manager distinguishes between single or multiple requestable products. Single request products are, for example, software, system roles, or Active Directory groups. These products cannot be requested if they have already been be requested for the same time period.

Furthermore, an identity may need several of one type of company resources, for example, consumables like pens or printer paper. You can find company resources such as these mapped in One Identity Manager as Multi-request resource or Multi requestable/unsubscribable resources.

The resources are assigned to identities after approval has been granted and they remain assigned until the request is unsubscribed. An example of multi requestable/unsubscribable resources would be printers or monitors.

You can perform a variety of actions on the multi requestable/unsubscribable resources that you manage and gather information about them.

Detailed information about this topic

- Displaying my multi requestable/unsubscribable resources on page 350
- Displaying my multi requestable/unsubscribable resources' overviews on page 351
- Displaying and editing my multi requestable/unsubscribable resources' main data on page 351
- My multi requestable/unsubscribable resources' memberships on page 352
- My multi requestable/unsubscribable resources' attestations on page 355

Displaying my multi requestable/unsubscribable resources

You can see all the multi requestable/unsubscribable resources for which you are responsible.

To display multi requestable/unsubscribable resources

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.

   This opens the **Multi requestable/unsubscribable Resources** page (see Multi requestable/unsubscribable resources (page description) on page 1154) and displays all the multi requestable/unsubscribable resources for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154

Displaying my multi requestable/unsubscribable resources' overviews

You can see all the relevant information about multi requestable/unsubscribable resources that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a multi requestable/unsubscribable resource's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <multi requestable/unsubscribable resource name>** page (see Overview – Multi requestable/unsubscribable resource (page description) on page 1156).

Related topics

- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154
- Multi requestable/unsubscribable resource overview page (page description) on page 1154
- Overview – Multi requestable/unsubscribable resource (page description) on page 1156

Displaying and editing my multi requestable/unsubscribable resources' main data

You can edit the main data of the multi requestable/unsubscribable resources for which you are responsible.

To display and edit a multi requestable/unsubscribable resource's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <multi requestable/unsubscribable resource name>**, make your changes in the respective fields (see Main data – Multi requestable/unsubscribable resource (page description) on page 1156).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154
- Multi requestable/unsubscribable resource overview page (page description) on page 1154
- Main data – Multi requestable/unsubscribable resource (page description) on page 1156

My multi requestable/unsubscribable resources' memberships

You can assign identities to multi requestable/unsubscribable resources for which you are responsible. You can see these identities, assign further identities to the multi requestable/unsubscribable resources and remove identities from the multi requestable/unsubscribable resources.

Detailed information about this topic

- Displaying my multi requestable/unsubscribable resources' memberships on page 353
- Assigning identities to my multi requestable/unsubscribable resources on page 353
- Removing identities from my multi requestable/unsubscribable resources on page 354

Displaying my multi requestable/unsubscribable resources' memberships

You can see identities that are assigned multi requestable/unsubscribable resources for which you are responsible.

To display identities that are assigned a multi requestable/unsubscribable resource

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <multi requestable/unsubscribable resource name>** page (see Memberships – Multi requestable/unsubscribable resource (page description) on page 1158).

Related topics

- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154
- Multi requestable/unsubscribable resource overview page (page description) on page 1154
- Memberships – Multi requestable/unsubscribable resource (page description) on page 1158

Assigning identities to my multi requestable/unsubscribable resources

You can assign identities to multi requestable/unsubscribable resources for which you are responsible. You do this through requests.

To assign an identity to a multi requestable/unsubscribable resource

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resources you want to assign an identity to.
4. On the overview page, click **Memberships**.

5. On the **Memberships - <multi requestable/unsubscribable resource name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the multi requestable/unsubscribable resource.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the multi requestable/unsubscribable resource.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154
- Multi requestable/unsubscribable resource overview page (page description) on page 1154
- Memberships – Multi requestable/unsubscribable resource (page description) on page 1158
- My shopping cart (page description) on page 869

Removing identities from my multi requestable/unsubscribable resources

You can remove identities from multi requestable/unsubscribable resources for which you are responsible.

To remove an identity from a multi requestable/unsubscribable resource

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resources you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <multi requestable/unsubscribable resource name>** page, select the check box next to the multi requestable/unsubscribable resource that you want to remove.
6. Click **Delete memberships**.

   This cancels the multi requestable/unsubscribable resource's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154
- Multi requestable/unsubscribable resource overview page (page description) on page 1154
- Memberships – Multi requestable/unsubscribable resource (page description) on page 1158

My multi requestable/unsubscribable resources' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my multi requestable/unsubscribable resources' attestation cases on page 356
- Displaying attestors of my multi requestable/unsubscribable resources' pending attestation cases on page 357
- Approving and denying my multi requestable/unsubscribable resources' attestation cases on page 358
- Sending reminders about my multi requestable/unsubscribable resources' pending attestation cases on page 359

Displaying my multi requestable/unsubscribable resources' attestation cases

You can see attestation cases that involve multi requestable/unsubscribable resources for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <multi requestable/unsubscribable resource name>** page (see Attestation – Multi requestable/unsubscribable resource (page description) on page 1159).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154
- Multi requestable/unsubscribable resource overview page (page description) on page 1154
- Attestation – Multi requestable/unsubscribable resource (page description) on page 1159

Displaying attestors of my multi requestable/unsubscribable resources' pending attestation cases

You can see identities that still have pending attestation cases from multi requestable/unsubscribable resources for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

5. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154
- Multi requestable/unsubscribable resource overview page (page description) on page 1154
- Attestation – Multi requestable/unsubscribable resource (page description) on page 1159

Approving and denying my multi requestable/unsubscribable resources' attestation cases

You can grant or deny approval to attestation cases of multi requestable/unsubscribable resources for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Attestation - <multi requestable/unsubscribable resource name>** page, perform one of the following actions:
   - Click (**Approve**) next to the attestation case you want to approve.
   - Click (**Deny**) next to the attestation case you want to deny.

   TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).

8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154
- Multi requestable/unsubscribable resource overview page (page description) on page 1154
- Attestation – Multi requestable/unsubscribable resource (page description) on page 1159

Sending reminders about my multi requestable/unsubscribable resources' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Multi requestable/unsubscribable resources (page description) on page 1154
- Multi requestable/unsubscribable resource overview page (page description) on page 1154
- Attestation – Multi requestable/unsubscribable resource (page description) on page 1159

Managing my resources

An identity can own resources just once and they can only be requested by them once. After being approved, they remain assigned until they are unsubscribed. You can request them again a later point. For example, a resource could be a telephone or a company car.

You can perform a variety of actions on resources that you manage and gather information about them.

Detailed information about this topic

- Displaying my resources on page 362
- Displaying my resources' overviews on page 362
- Creating your own resources on page 363
- Displaying and editing my resources' main data on page 363

- My resources' memberships on page 364
- My resources' attestations on page 366
- Displaying role memberships of my resources' members on page 371

Displaying my resources

You can see all the resources for which you are responsible.

To display resources

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.

   This opens the **Resources** page (see Resources (page description) on page 1129) and displays all the resources for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129

Displaying my resources' overviews

You can see all the relevant information about resources that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a resource's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <resource name>** page (see Overview – Resource (page description) on page 1132).

Related topics

- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Overview – Resource (page description) on page 1132

Creating your own resources

You can create new resources for which you are responsible.

To create a new resource

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click **New resource**.
4. On the **New resource** page, enter the resource's main data in the respective fields (see New resources (page description) on page 1129).
5. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- New resources (page description) on page 1129

Displaying and editing my resources' main data

You can edit the main data of the resources for which you are responsible.

To display and edit a resource's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <resource name>**, make your changes in the respective fields (see Main data – Resource (page description) on page 1132).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Main data – Resource (page description) on page 1132

My resources' memberships

You can assign identities to resources for which you are responsible. You can see these identities, assign further identities to the resources and remove identities from the resources.

Detailed information about this topic

- Displaying memberships in my resources on page 364
- Assigning identities to my resources on page 364
- Removing identities from my resources on page 365

Displaying memberships in my resources

You can see identities that are assigned resources for which you are responsible.

To display identities that are assigned a resource

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <resource name>** page (see Memberships – Resource (page description) on page 1133).

Related topics

- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Memberships – Resource (page description) on page 1133

Assigning identities to my resources

You can assign identities to resources for which you are responsible. You do this through requests.

To assign an identity to a resource

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource you want to assign an identity to.

4. On the overview page, click **Memberships**.
5. On the **Memberships - <resource name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the resource.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the resource.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Memberships – Resource (page description) on page 1133
- My shopping cart (page description) on page 869

Removing identities from my resources

You can remove identities from resources for which you are responsible.

To remove an identity from a resource

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <resource name>** page, select the check box next to the resource that you want to remove.
6. Click **Delete memberships**.

   This cancels the resource's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Memberships – Resource (page description) on page 1133

My resources' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my resources' attestation cases on page 366
- Displaying attestors of my resources' pending attestation cases on page 367
- Approving and denying my resources' attestation cases on page 368
- Sending reminders about my resources' pending attestation cases on page 370

Displaying my resources' attestation cases

You can see attestation cases that involve resources for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <resource name>** page (see Attestation - Resource (page description) on page 1134).
5. (Optional) Click on a tab to display the respective attestation cases.

6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click **show details**.
    c. In the **Attested object** dialog, select an object in the **Object** menu.

       This shows information about the object.
    d. (Optional) Click **View current state of the object**

       This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click the **History** tab.

       This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Attestation - Resource (page description) on page 1134

Displaying attestors of my resources' pending attestation cases

You can see identities that still have pending attestation cases from resources for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

5. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Attestation - Resource (page description) on page 1134

Approving and denying my resources' attestation cases

You can grant or deny approval to attestation cases of resources for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.

5. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Attestation - <resource name>** page, perform one of the following actions:
    - Click ☑ (**Approve**) next to the attestation case you want to approve.
    - Click ☒ (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Attestation - Resource (page description) on page 1134

Sending reminders about my resources' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.

6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Attestation - Resource (page description) on page 1134

Displaying role memberships of my resources' members

You can display the roles and organizations belonging to identities that are assigned resources for which you are responsible. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a resource

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Resources**.

3. On the **Resources** page, click the resource whose members you want to know more about.
4. On the overview page, click **Usage**.

   This opens the **Usage - <resource name>** page (see Usage – Resource (page description) on page 1136).
5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- My responsibilities (page description) on page 1014
- Resources (page description) on page 1129
- Resource overview page (page description) on page 1130
- Usage – Resource (page description) on page 1136

Managing my software applications

Software applications can be assigned directly or indirectly to identities. Indirect assignment is carried out by allocating identities and software applications in company structures, like departments, cost centers, locations, or business roles. Examples of software application that can be assigned are: internet, address management, email or text editing software.

You can perform a variety of actions on the software applications that you manage and gather information about them.

Detailed information about this topic

- Displaying my software applications on page 373
- Adding your own software on page 373
- Displaying my software applications' overviews on page 373
- Displaying and editing my software applications' main data on page 374
- My software applications' memberships on page 375
- My software applications' attestations on page 377
- Displaying role memberships of my software applications' members on page 383

Displaying my software applications

You can see all the software applications for which you are responsible.

To display software applications

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.

   This opens the **Software** page (see Software (page description) on page 1146) and displays all the software applications for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Software (page description) on page 1146

Adding your own software

You can create new software applications for which you are responsible.

To create a new software application

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click **New software**.
4. On the **New software** page, enter the software's main data in the respective fields (see New software (page description) on page 1147).
5. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- New software (page description) on page 1147

Displaying my software applications' overviews

You can see all the relevant information about software applications that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a software application's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <software application name>** page (see Overview - Software (page description) on page 1149).

Related topics

- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Overview - Software (page description) on page 1149

Displaying and editing my software applications' main data

You can edit the main data of the software applications for which you are responsible.

To display and edit a software application's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <software application name>**, make your changes in the respective fields (see Main data - Software (page description) on page 1149).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Main data - Software (page description) on page 1149

My software applications' memberships

You can assign identities to software application for which you are responsible. You can see these identities, assign further identities to the software applications and remove identities from the software applications.

Detailed information about this topic

- Displaying memberships in my software applications on page 375
- Assigning identities to my software applications on page 375
- Removing identities from my software applications on page 376

Displaying memberships in my software applications

You can see identities that are assigned software application for which you are responsible.

To display identities that are assigned a software application

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <software application name>** page (see Memberships – Software (page description) on page 1150).

Related topics

- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Memberships – Software (page description) on page 1150

Assigning identities to my software applications

You can assign identities to software applications for which you are responsible. You do this through requests.

To assign an identity to a software application

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.

3. On the **Software** page, click the software application you want to assign an identity to.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <software application name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the software application.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   > TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the software application.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Memberships – Software (page description) on page 1150
- My shopping cart (page description) on page 869

Removing identities from my software applications

You can remove identities from software applications for which you are responsible.

To remove an identity from a software application

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <software application name>** page, select the check box next to the software application that you want to remove.
6. Click **Delete memberships**.

   This cancels the software application's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Memberships – Software (page description) on page 1150

My software applications' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my software applications' attestation cases on page 377
- Displaying attestors of my software applications' pending attestation cases on page 379
- Approving and denying my software applications' attestation cases on page 380
- Sending reminders about my software applications' pending attestation cases on page 381

Displaying my software applications' attestation cases

You can see attestation cases that involve software application for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <software application name>** page (see Attestation – Software (page description) on page 1152).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Attestation – Software (page description) on page 1152

Displaying attestors of my software applications' pending attestation cases

You can see identities that still have pending attestation cases from software applications for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <software application name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <software application name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Attestation – Software (page description) on page 1152

Approving and denying my software applications' attestation cases

You can grant or deny approval to attestation cases of software applications entitlements for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <software application name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Attestation - <software application name>** page, perform one of the following actions:
   - Click ☑ (**Approve**) next to the attestation case you want to approve.
   - Click ☒ (**Deny**) next to the attestation case you want to deny.

   TIP: To grant or deny approval for all the attestation cases displayed, click ☑ (**Approve all**) or ☒ (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
   - For approved attestation case:
     - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
   - For denied attestation cases:
     - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
     - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
   - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

   TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Attestation – Software (page description) on page 1152

Sending reminders about my software applications' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <software application name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

This opens an email template with the attestor's email address.

10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <software application name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <software application name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Attestation – Software (page description) on page 1152

Displaying role memberships of my software applications' members

You can display the roles and organizations belonging to identities that are assigned software applications for which you are responsible. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a software application

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Software**.
3. On the **Software** page, click the software application whose members you want to know more about.
4. On the overview page, click **Usage**.

   This opens the **Usage - <software application name>** page (see Usage – Software (page description) on page 1153).
5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- My responsibilities (page description) on page 1014
- Software (page description) on page 1146
- Software application overview page (page description) on page 1148
- Usage – Software (page description) on page 1153

Managing my locations

You can perform a variety of actions on locations that you manage and gather information about them.

Detailed information about this topic

- Displaying my locations on page 384
- Restoring my deleted locations on page 384
- Displaying my locations' overviews on page 385

- Displaying and editing my locations' main data on page 386
- My locations' memberships on page 386
- My locations' entitlements on page 389
- My locations' attestations on page 391
- Compliance: My locations on page 396
- Displaying my locations' risk indexes on page 399
- My locations' history on page 400
- Displaying role memberships of my locations' members on page 403
- Copying/splitting my locations on page 404
- Comparing and merging my locations on page 405
- Displaying my locations' statistics on page 406

Displaying my locations

You can see all the locations for which you are responsible.

To display locations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.

   This opens the **Locations** page (see Locations (page description) on page 1102) and displays all the locations for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102

Restoring my deleted locations

You can recover deleted locations for which you were responsible. For example, a location can be deleted if two roles are merged during comparison (see Comparing and merging my locations on page 405).

To restore a deleted location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click **Restore a deleted role**.

4. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the location was deleted.
5. Next to the location you want to restore, select the check box.
6. Click **Next**.
7. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
8. Click **Next**.
9. Click **Close**.

To restore a deleted child location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location that was originally parent to the deleted location.
4. On the overview page, click **Restore**.
5. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the location was deleted.
6. In the list next to the location you want to restore, select the check box.
7. Click **Next**.
8. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
9. Click **Next**.
10. Click **Close**.

Related topics

- Comparing and merging my locations on page 405
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103

Displaying my locations' overviews

You can see all the relevant information about locations that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a location's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <location name>** page (see Overview - Location (page description) on page 1106).

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Overview - Location (page description) on page 1106

Displaying and editing my locations' main data

You can edit the main data of the locations for which you are responsible.

To display and edit a location's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the locations whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <location name>**, make your changes in the respective fields (see Main data - Location (page description) on page 1106).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Main data - Location (page description) on page 1106

My locations' memberships

You can assign identities to locations for which you are responsible. You can see these identities, assign further identities to the locations and remove identities from the locations.

Detailed information about this topic

- Displaying memberships in my locations on page 387
- Assigning identities to my locations on page 387
- Removing identities from my locations on page 388

Displaying memberships in my locations

You can see identities that are assigned locations for which you are responsible.

To display identities that are assigned a location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <location name>** page (see Memberships – Location (page description) on page 1107).

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Memberships – Location (page description) on page 1107

Assigning identities to my locations

You can assign identities to locations for which you are responsible. You do this through requests.

To assign an identity to an application role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location you want to assign an identity to.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <location name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the location.

7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the location.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Memberships – Location (page description) on page 1107
- My shopping cart (page description) on page 869

Removing identities from my locations

You can remove identities from locations for which you are responsible.

To remove an identity from a location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <location name>** page, select the check box next to the location that you want to remove.
6. Click **Delete memberships**.

   This cancels the location's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Memberships – Location (page description) on page 1107

My locations' entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to a location you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the location.

Detailed information about this topic

- Displaying my locations' entitlements on page 389
- Adding my locations' entitlements on page 390
- Deleting my locations' entitlements on page 390

Displaying my locations' entitlements

You can see entitlements that are assigned locations for which you are responsible. You can also display the reason why locations have certain entitlements (entitlement origin).

To display a location's entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <location name>** page (see Entitlements – Location (page description) on page 1108).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Entitlements – Location (page description) on page 1108

Adding my locations' entitlements

You can add entitlements to locations for which you are responsible. You do this through requests.

To assign an entitlement to a location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location to which you want to add an entitlement.
4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <location name>** page, click **Add new**.
6. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
7. Click **Assign**.
8. In the **Entitlement** dialog, in the list, click the entitlement that you want to add to the business role.
9. In the **Add a new entitlement** dialog, click **Request**.
10. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    After the request has been granted approval, the entitlement is added to the location.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Entitlements – Location (page description) on page 1108

Deleting my locations' entitlements

You can delete entitlements that are assigned locations for which you are responsible.

To delete an entitlement of a location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose entitlements you want to delete.

4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <location name>** page, in the list, select the check box in the row of the entitlement you want to delete.
6. Click **Delete**.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Entitlements – Location (page description) on page 1108

My locations' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my locations' attestation cases on page 391
- Displaying attestors of my locations' pending attestation cases on page 393
- Approving and denying my locations' attestation cases on page 394
- Sending reminders about my locations' pending attestation cases on page 395

Displaying my locations' attestation cases

You can see attestation cases that involve locations for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <location name>** page (see Attestation – Location (page description) on page 1110).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Attestation – Location (page description) on page 1110

Displaying attestors of my locations' pending attestation cases

You can see identities that still have pending attestation cases from locations for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Attestation – Location (page description) on page 1110

Approving and denying my locations' attestation cases

You can grant or deny approval to attestation cases of locations for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Attestation - <location name>** page, perform one of the following actions:
    - Click ☑ (**Approve**) next to the attestation case you want to approve.
    - Click ☒ (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Attestation – Location (page description) on page 1110

Sending reminders about my locations' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the locations whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the locations whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the locations whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Attestation – Location (page description) on page 1110

Compliance: My locations

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying my locations' rule violations on page 397
- Displaying my locations' policy violations on page 398
- Displaying rule violations of my locations' members on page 398
- Displaying risk indexes and entitlements of my locations' members on page 399

Displaying my locations' rule violations

You can see the rule violations of locations for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose rule violations you want to display.
4. On the overview page, click **Compliance**.

   This opens the **Compliance - <location name>** page (see Compliance – Location (page description) on page 1109).

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Compliance – Location (page description) on page 1109

Displaying my locations' policy violations

You can see the policy violations of locations for which you are responsible.

To display policy violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose policy violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <location name>** page (see Compliance reports - Location (page description) on page 1115).
5. In the **View** menu, select **Policy violations**.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Compliance reports - Location (page description) on page 1115

Displaying rule violations of my locations' members

You can see the rule violations of identities that are assigned locations for which you are responsible.

To display rule violations of a location's members

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose rule violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <location name>** page (see Compliance reports - Location (page description) on page 1115).

5. In the **View** menu, select **Compliance rule violations**.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Compliance reports - Location (page description) on page 1115

Displaying risk indexes and entitlements of my locations' members

For every location that you are responsible for, you can see all the identities that have these location as primary or secondary assignments. You can also display the number of permissions assigned and the risk index.

To display members of a location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose members you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <location name>** page (see Compliance reports - Location (page description) on page 1115).
5. In the **View** menu, select **Identities: Risk indexes and entitlements**.
6. (Optional) To display more information about an identity, perform the following actions:
   a. In the list, click an identity.
   b. In the dialog, click **Overview**.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Compliance reports - Location (page description) on page 1115

Displaying my locations' risk indexes

You can see risk indexes of locations for which you are responsible.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a cost center's risk index

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose risk index you want to display.
4. On the overview page, click **Risk**.

   This opens the **Risk - <location name>** page (see Risk – Location (page description) on page 1111).
5. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Risk – Location (page description) on page 1111

My locations' history

The Web Portal gives you the option of displaying the historical data of locations for which you are responsible.

To do this, you have the following options:

Table 32: Historical data

View	Description
Events	This shows you all the events that affect the location, either on a timeline or in a table (see Displaying my locations' history on page 401).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my locations on page 402).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was

View	Description
	at the selected point in time and what the value is now (see Comparing statuses of my locations on page 402).

Displaying my locations' history

You can see all the events affecting locations that you are responsible for, either on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <location name>** page (see History – Location (page description) on page 1112).

   TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

   To zoom in or out, turn the mouse wheel.
5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- History – Location (page description) on page 1112

Displaying the status overview of my locations

You can display all the changes effecting locations for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <location name>** page (see History – Location (page description) on page 1112).
5. Click the **Status overview** tab.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- History – Location (page description) on page 1112

Comparing statuses of my locations

You can compare the current status of a location that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose status you want to compare.
4. On the overview page, click **History**.

5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since creation, deselect the check box next to **Display changed values only**.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- History – Location (page description) on page 1112

Displaying role memberships of my locations' members

You can display the roles and organizations belonging to identities that are assigned locations for which you are responsible. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose members you want to know more about.
4. On the overview page, click **Usage**.

This opens the **Usage - <location name>** page (see Usage – Location (page description) on page 1114).

5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103
- Usage – Location (page description) on page 1114

Copying/splitting my locations

You can copy or move memberships and entitlements from locations you are responsible for to new roles (departments, business roles, cost centers, locations).

Any combination of role types is allowed.

To copy a location or move memberships and entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location you want to copy or whose memberships and entitlements you want to move.
4. On the overview page, click **Split**.
5. In the **Split a role** dialog, in the **Type of the new role** menu, select a type for the new role.
6. Depending on which role type you have selected, enter the corresponding main data of the new role (see Main data – Department (page description) on page 1079, Main data – Business role (page description) on page 1050, Main data – Cost center (page description) on page 1093, or Main data - Location (page description) on page 1106).
7. Click **Next**.
8. Perform the following actions:
    - To neither copy nor move a entitlement/membership to a new role, click **Actions** > **Keep this assignment** next to the corresponding entitlement/membership. Later, the entitlement/membership is only available in the source role.

- To copy a entitlement/membership to a new role, click **Actions** > **Keep and copy to new role** next to the corresponding entitlement/membership. The entitlement/membership is later included in the source role as well as the target role.
- To move a entitlement/membership to a new role, click **Actions** > **Move to new role** next to the corresponding entitlement/membership. The entitlement/membership is later removed from the source role and is only included in the target role.

9. Click **Next**.
10. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.
12. Click **Close**.

Related topics

- My locations' memberships on page 386
- My locations' entitlements on page 389
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103

Comparing and merging my locations

You can compare properties of locations that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a location

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location you want to compare and merge.
4. On the overview page, click **Compare and merge**.
5. In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your location.
6. Click **Assign**.
7. In the **Comparison role** dialog, select the business role/department/cost center/location to compare.

   The assigned memberships and entitlements of both objects are listed with the following information:

Table 33: Overview of the assignments

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Object</td><td>Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.</td></tr>
<tr><td>Type</td><td>Type of the entitlement/membership.</td></tr>
<tr><td><Name of the source object></td><td rowspan="2">Shows you the entitlement/membership's assignment type. The following assignment types are available.
• Direct
• Inherited
• Requested
• Dynamic
• Not assigned
For more detailed information about assigning company resources, see the One Identity Manager Identity Management Base Module Administration Guide.</td></tr>
<tr><td><Name of the compare object></td></tr>
<tr><td>Comparison</td><td>Shows you where the entitlement/membership occurs.</td></tr>
</table>

> TIP: To arrange the list of assignments better, use the filters available some of the columns. For more information, see Filtering on page 40..

8. In the **Compare and merge** dialog, click **Merge the selected roles**.
9. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
10. Click **Next**.
11. Click **Close**.

Related topics

- My locations' memberships on page 386
- My locations' entitlements on page 389
- My responsibilities (page description) on page 1014
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103

Displaying my locations' statistics

You can see statistics of locations for which you are responsible.

To display a location's statistics

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Locations**.
3. On the **Locations** page, click the location whose statistics you want to display.
4. On the overview page, click **Statistics**.

   This opens the **Statistics for <location name>** dialog and shows the location's statistics.
5. (Optional) To obtain more information about a chart, click the chart or its header.

Related topics

- Discovering your statistics on the home page on page 795
- Statistics on page 795
- Locations (page description) on page 1102
- Location overview page (page description) on page 1103

Managing my system entitlements

System entitlements map the objects that control access to target system resources in the target systems. A user account obtains the required permissions for accessing target system resources through its memberships in system entitlements.

You can carry out various actions on the system entitlements that you manage and obtain information about them.

You could manage the following system entitlements:

- Active Directory groups
- SAP groups
- SharePoint groups
- PAM groups

Detailed information about this topic

- Displaying my system entitlements on page 408
- Displaying my system entitlements' overviews on page 408
- Displaying and editing my system entitlements main data on page 409
- Deleting my Active Directory groups on page 410
- My system entitlements' memberships on page 411
- My system entitlement's child groups on page 414
- My system entitlements' attestations on page 416

- My system entitlements' product owners on page 423
- My system entitlements' history on page 426
- Displaying role memberships of my system entitlements' members on page 429

Displaying my system entitlements

You can see all the system entitlements for which you are responsible.

To display system entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.

   This opens the **System Entitlements** page (see System entitlements (page description) on page 1032) and displays all the system entitlements for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032

Displaying my system entitlements' overviews

You can see all the relevant information about system entitlements that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a system entitlement's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <system entitlement name>** page (see Overview – System entitlement (page description) on page 1035).

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032

- System entitlement overview page (page description) on page 1033
- Overview – System entitlement (page description) on page 1035

Displaying and editing my system entitlements main data

You can edit the main data of the system entitlements for which you are responsible.

To display and edit a system entitlement's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlements whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <system entitlement name>**, make your changes in the respective fields (see Main data – System entitlement (page description) on page 1035).
6. Click **Save**.

To edit the group scope and group type of an Active Directory group

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the Active Directory that you want to edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <Active Directory group name>**, click **Request modification**.
6. In the **Modify Active Directory group** dialog, make your changes in the respective fields:
    - **Group scope**: Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can specify one of the following group scopes:
        - **Global group**: Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group’s domain.
        - **Local**: Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.

    - **Universal**: Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
  - **Group type**: Specify whether this is an Active Directory security group or an Active Directory distribution group.
7. Click **OK**.
8. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   The Active Directory group changes after the modifications to the Active Directory group have been granted approval.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Main data – System entitlement (page description) on page 1035
- My shopping cart (page description) on page 869

Deleting my Active Directory groups

You cannot directly delete Active Directory groups for which you are responsible. You can request deletion of the Active Directory groups and await approval of the request.

To delete Active Directory groups

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the Active Directory group that you want to delete.
4. On the overview page, click **Main data**.
5. On the **Main data - <Active Directory group name>**, click **Request deletion**.
6. In the dialog, confirm the prompt with **Yes**.
7. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   The Active Directory group is deleted after it has been granted approval.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Main data – System entitlement (page description) on page 1035
- My shopping cart (page description) on page 869

Specifying my system entitlement owners

You can specify which identities are responsible for your system entitlements. To do this, you must assign one or more product owners to the service item assigned to the system entitlement.

To specify owners for a system entitlement

1.
2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose owners you want to specify.
4. In the **Edit System Entitlement** pane, click the **Service Item** tab.
5. On the **Service Item** tab, perform one of the following actions:
    - To specify members of a specific application role as product owners, perform the following under **Product owners**:
        1. Enable the **Select from roles** option.
        2. In the **Product owner** field, click **Assign/Change**.
        3. In the **Edit Product Owner** pane, click the appropriate application role.
    - To specify a specific identity as the product owner, perform the following under **Product owners**:
        1. Enable the **Select from identities** option.
        2. In the **Identity** list, select the corresponding identity.
6. Click **Save**.

My system entitlements' memberships

You can assign identities to system entitlements for which you are responsible. You can see these identities, assign further identities to the system entitlements and remove identities from the system entitlements.

Detailed information about this topic

- Displaying memberships in my system entitlements on page 412
- Assigning identities to my system entitlements on page 412
- Removing identities from my system entitlements on page 413

Displaying memberships in my system entitlements

You can see identities that are assigned system entitlements for which you are responsible.

To display identities that are assigned a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <system entitlement name>** page (see Memberships – System entitlement (page description) on page 1037).

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Memberships – System entitlement (page description) on page 1037

Assigning identities to my system entitlements

You can assign identities to system entitlements for which you are responsible. You do this through requests.

To assign an identity to a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement you want to assign an identity to.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <system entitlement name>** page, click **Request memberships**.

6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the system entitlement.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the system entitlement.

Related topics

- Requesting products on page 86
- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Memberships – System entitlement (page description) on page 1037
- My shopping cart (page description) on page 869

Removing identities from my system entitlements

You can remove identities from system entitlements for which you are responsible.

To remove an identity from a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <system entitlement name>** page, select the check box next to the system entitlements that you want to remove.
6. Click **Delete memberships**.

   This cancels the system entitlement's assignment.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Memberships – System entitlement (page description) on page 1037

My system entitlement's child groups

You can order more groups under certain group types or order these under other groups:

- Active Directory groups
- LDAP groups
- Notes groups
- Custom target systems groups

Detailed information about this topic

- Display my system entitlements' child groups on page 414
- Assigning child groups to my system entitlements on page 414
- To remove child groups from my system entitlements on page 415

Display my system entitlements' child groups

You can see all groups that are child groups of the system entitlements for which you are responsible.

To display the child groups of a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose child groups you want to display.
4. On the overview page, click **Child groups**.

   This opens the **Child groups - <system entitlement name>** page (see Child groups – System entitlement (page description) on page 1038).

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Child groups – System entitlement (page description) on page 1038

Assigning child groups to my system entitlements

You can assign child groups to system entitlements for which you are responsible.

To assign a child group to a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement you want to assign a child group to.
4. On the overview page, click **Child groups**.
5. On the **Child groups - <system entitlement name>**, click **New child group**.
6. In the **Add members group** dialog, click **Assign**.
7. In the **Child group** dialog, in the list, click the group you want to add to the system entitlement.
8. In the **Add members group** dialog, click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Child groups – System entitlement (page description) on page 1038

To remove child groups from my system entitlements

You can remove the child groups of the system entitlements for which you are responsible.

To remove a child group from a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose child groups you want to remove.
4. On the overview page, click **Child groups**.
5. On the **Child groups - <system entitlement name>** page, in the list, select the check box in the row of the child group that you want to remove.
6. Click **Remove selected**.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Child groups – System entitlement (page description) on page 1038

My system entitlements' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my system entitlements' attestation cases on page 416
- Displaying attestors of my system entitlements' pending attestation cases on page 417
- Approving and denying my system entitlements' attestation cases on page 418
- Sending reminders about my system entitlements' pending attestation cases on page 420
- My system entitlements' attestors on page 421

Displaying my system entitlements' attestation cases

You can see attestation cases that involve system entitlements for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

This opens the **Attestation - <system entitlement name>** page (see Attestation – System entitlement (page description) on page 1039).

5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Attestation – System entitlement (page description) on page 1039

Displaying attestors of my system entitlements' pending attestation cases

You can see identities that still have pending attestation cases from system entitlements for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Attestation – System entitlement (page description) on page 1039

Approving and denying my system entitlements' attestation cases

You can grant or deny approval to attestation cases of system entitlements for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
6. Click **Approve**.
7. On the **Pending Attestations - <system entitlement name>** page, perform one of the following actions:
    - Click ☑ (**Approve**) next to the attestation case you want to approve.
    - Click ☒ (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Attestation – System entitlement (page description) on page 1039

Sending reminders about my system entitlements' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases.

6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Attestation – System entitlement (page description) on page 1039

My system entitlements' attestors

Identities that can approve attestation cases of system entitlements are assigned as attestors through application roles.

Detailed information about this topic

- Displaying my system entitlements' attestors on page 421
- Specifying attestors for my system entitlements on page 422

Displaying my system entitlements' attestors

You can display which identities can attest system entitlements for which you are responsible.

To display attestors of a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestor you want to display.
4. On the overview page, click **Attestors**.

   This opens the **Attestors - <system entitlement name>** page (see Attestors – System entitlement (page description) on page 1041). In the details pane, under **Assigned**, all the identities to which the assigned application role is assigned are displayed. These identities can approve system entitlement attestation cases.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Attestors – System entitlement (page description) on page 1041

Specifying attestors for my system entitlements

You can specify identities that can approve the attestation cases of system entitlements for which you are responsible.

To specify attestors for a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestor you want to specify.
4. On the overview page, click **Attestors**.
5. On the **Attestors - <system entitlement name>** page, perform one of the following actions:
   a. Next to **Attestor**, click **Assign/Change**.
   b. In the **Attestors** dialog, click an application role in the list whose members can approve the system entitlement's attestation cases.
6. (Optional) To assign additional identities to the application role so that those identities can approve the system entitlement attestation case, click the appropriate identities in the list.
7. Click **Save**.

To create a new attestor role for a system entitlement and assign it.

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestor you want to specify.
4. On the overview page, click **Attestors**.
5. On the **Attestors - <system entitlement name>** page, click **Add new**.
6. In the **Create new attestor application role** dialog, enter additional information about the new application role:
   - **Application role**: Enter a name for the new application role.
   - **Description**: (Optional) Enter a description for the new application role.
7. Click **Save**.
8. On the **Attestors - <name of system entitlement>** page, in the list, click the identities that can approve the system entitlement's attestation cases. This assigns the identities to the application role.
9. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Attestors – System entitlement (page description) on page 1041

My system entitlements' product owners

Identities responsible for system entitlements are assigned as owners through application roles.

Detailed information about this topic

- Displaying my system entitlements' product owners on page 423
- Specifying product owners for my system entitlements on page 424

Displaying my system entitlements' product owners

You can display identities that are responsible for system entitlements for which you are also responsible.

To display the owners of a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose owners you want to display.
4. On the overview page click **Owners**.

   This opens the **Owners - <system entitlement name>** page (see Owners – System entitlement (page description) on page 1042). In the details pane, under **Assigned**, all the identities to which the assigned application role is assigned are displayed. These identities are responsible for the system entitlement.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Owners – System entitlement (page description) on page 1042

Specifying product owners for my system entitlements

You can specify which identities are responsible for system entitlements for which you are also responsible.

To specify owners for a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose product owner you want to specify.
4. On the overview page click **Owners**.
5. On the **Owners - <system entitlement name>** page, perform one of the following actions:
   a. Next to **Product owner**, click **Assign**/**Change**.
   b. In the **Product owner** dialog, in the list, click an application role whose members are responsible for the system entitlement.
6. (Optional) To assign the application role to additional identities so that those identities are responsible for system entitlement, click the appropriate identities in the list.
7. Click **Save**.

To create and assign a new owner role for a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose owners you want to specify.
4. On the overview page click **Owners**.
5. On the **Owners - <system entitlement name>** page, click **Add new**.
6. In the **Create new owner role** dialog, enter additional information about the new application role:
    - **Application role**: Enter a name for the new application role.
    - **Description**: (Optional) Enter a description for the new application role.
7. Click **Save**.
8. On the **Owners - <system entitlement name>** page, in the list, click the identities that will be responsible for the system entitlement. This assigns the identities to the application role.
9. Click **Save**.

To create and assign a new owner role with the same members as the currently selected owner role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose owners you want to specify.
4. On the overview page click **Owners**.
5. On the **Owners - <system entitlement name>** page, click **Move ownership**.
6. In the **Move ownership to new owner role** dialog, select the check box next to **Move all owners**.
7. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Owners – System entitlement (page description) on page 1042

My system entitlements' history

The Web Portal gives you the option of displaying the historical data of system entitlements for which you are responsible.

To do this, you have the following options:

Table 34: Historical data

View	Description
Events	This shows you all the events that affect the system entitlement, either on a timeline or in a table (see Displaying my system entitlements' history on page 426).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status my system entitlements' overview on page 427).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my system entitlements on page 428).

Displaying my system entitlements' history

You can see all the events affecting system entitlements that you are responsible for, either on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <system entitlement name>** page (see History – System entitlement (page description) on page 1043).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.
5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:

- **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
- **Change type**: Only show events on the timeline with the selected change type.
- **Date**: Only show events on the timeline that took place in the given period.
- **Properties**: Only show events on the timeline with the selected properties.
- **Display**: Only show events on the timeline that match the search.
- **Object**: Only show events on the timeline about the selected object.

6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- History – System entitlement (page description) on page 1043

Displaying the status my system entitlements' overview

You can see all the changes effecting system entitlements for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <system entitlement name>** page (see History – System entitlement (page description) on page 1043).
5. Click the **Status overview** tab.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- History – System entitlement (page description) on page 1043

Comparing statuses of my system entitlements

You can compare the current status of a system entitlement that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since creation, deselect the check box next to **Display changed values only**.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- History – System entitlement (page description) on page 1043

Displaying role memberships of my system entitlements' members

You can display the roles and organizations belonging to identities that are assigned system entitlements for which you are responsible. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a system entitlement

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose members you want to know more about.
4. On the overview page, click **Usage**.

   This opens the **Usage - <system entitlement name>** page (see Usage – System entitlement (page description) on page 1045).
5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- My responsibilities (page description) on page 1014
- System entitlements (page description) on page 1032
- System entitlement overview page (page description) on page 1033
- Usage – System entitlement (page description) on page 1045

Managing my system roles

System roles combine company resources that must always be assigned to identities together into a single package. Different types of company resources can be grouped into one system role, such as Active Directory groups, software, and resources. System roles can be assigned to user accounts, requested, or inherited through hierarchical roles. Employees and workdesks inherit company resources assigned to the system roles.

You can perform a variety of actions regarding system roles that you manage and gather information about them.

Detailed information about this topic

- Displaying my system roles on page 430
- Creating your own system roles on page 431
- Displaying my system roles' overviews on page 431
- Displaying and editing my system roles' main data on page 432
- My system roles' memberships on page 432
- My system roles' entitlements on page 434
- Compliance: My system roles on page 437
- My system roles' attestations on page 440
- Displaying my system roles' risk indexes on page 446
- My system roles' history on page 446
- Displaying role memberships of my system roles' members on page 449

Displaying my system roles

You can see all the system roles for which you are responsible.

To display system roles

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.

   This opens the **System Roles** page (see System roles (page description) on page 1061) and displays all the system roles for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061

Creating your own system roles

You can create new system roles for which you are responsible.

To create a new system role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System roles** page, click **New system role**.
4. On the **New system role** page, enter the system role's main data in the respective fields (see New system role (page description) on page 1062).
5. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- New system role (page description) on page 1062

Displaying my system roles' overviews

You can see all the relevant information about system roles that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display a system role's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <system role name>** page (see Overview – System role (page description) on page 1065).

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Overview – System role (page description) on page 1065

Displaying and editing my system roles' main data

You can edit the main data of the system roles for which you are responsible.

To display and edit a system role's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose main data you want to display.
4. On the overview page, click **Main data**.
5. On the **Main data - <system role name>**, make your changes in the respective fields (see Main data – System role (page description) on page 1065).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Main data – System role (page description) on page 1065

My system roles' memberships

You can assign identities to system roles for which you are responsible. You can see these identities, assign further identities to the system roles and remove identities from the system roles.

Detailed information about this topic

- Displaying memberships in my system roles on page 432
- Assigning identities to my system roles on page 433
- Removing identities from my system roles on page 434

Displaying memberships in my system roles

You can see identities that are assigned system roles for which you are responsible.

To display identities that are assigned a system role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.

3. On the **System Roles** page, click the system role whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <system role name>** page (see Memberships – System role (page description) on page 1067).

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Memberships – System role (page description) on page 1067

Assigning identities to my system roles

You can assign identities to system roles for which you are responsible. You do this through requests.

To assign an identity to a system role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role you want to assign an identity to.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <system role name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the system role.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   > TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the system role.

Related topics

- Requesting products on page 86
- My responsibilities on page 218
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063

- Memberships – System role (page description) on page 1067
- My shopping cart (page description) on page 869

Removing identities from my system roles

You can remove identities from system roles for which you are responsible.

To remove an identity from a system role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <system role name>** page, select the check box next to the system role that you want to remove.
6. Click **Delete memberships**.

   This cancels the system role's assignment.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Memberships – System role (page description) on page 1067

My system roles' entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. Assigning identities to system roles avoids you having to assign entitlements separately to each identity. All a system role's entitlements are automatically assigned to all the identities assigned to the system role.

Detailed information about this topic

- Displaying my system roles' entitlements on page 435
- Adding my system roles' entitlements on page 435
- Deleting my system roles' entitlements on page 436

Displaying my system roles' entitlements

You can see entitlements that are assigned system roles for which you are responsible. You can also display the reason why system roles have certain entitlements (entitlement origin).

To display a system role's entitlements

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <system role name>** page (see Entitlements – System role (page description) on page 1066).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Entitlements – System role (page description) on page 1066

Adding my system roles' entitlements

You can add entitlements to system roles for which you are responsible. You do this through requests.

To assign an entitlement to a system role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role to which you want to add an entitlement.
4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <system role name>** page, click **Add new**.

6. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
7. Click **Assign**.
8. In the **Entitlement** dialog, in the list, click the entitlement that you want to add to the business role.
9. In the **Add a new entitlement** dialog, click **Request**.
10. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    After the request has been granted approval, the entitlement is added to the system role.

Related topics

- Requesting products
- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Entitlements – System role (page description) on page 1066
- My shopping cart (page description) on page 869

Deleting my system roles' entitlements

You can delete entitlements that are assigned system roles for which you are responsible.

To delete an entitlement of a system role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose entitlements you want to delete.
4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <system role name>** page, in the list, select the check box in the row of the entitlement you want to delete.
6. Click **Delete**.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061

- System role overview page (page description) on page 1063
- Entitlements – System role (page description) on page 1066

Compliance: My system roles

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying my system roles' rule violations on page 437
- Displaying my system roles' policy violations on page 438
- Displaying rule violations of my system roles' members on page 438
- Displaying risk indexes and entitlements of my system roles' members on page 439

Displaying my system roles' rule violations

You can see the rule violations of system roles for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.

3. On the **System Roles** page, click the system role whose rule violations you want to display.
4. On the overview page, click **Compliance**.

   This opens the **Compliance - <system role name>** page (see Compliance – System role (page description) on page 1068).

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Compliance – System role (page description) on page 1068

Displaying my system roles' policy violations

You can see the policy violations of system roles for which you are responsible.

To display policy violations

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose policy violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <system role name>** page (see Compliance reports – system role (page description) on page 1074).
5. In the **View** menu, select **Policy violations**.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Compliance reports – system role (page description) on page 1074

Displaying rule violations of my system roles' members

You can see the rule violations of identities that are assigned system roles for which you are responsible.

To display rule violations of a system role's members

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose rule violations you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <system role name>** page (see Compliance reports – system role (page description) on page 1074).
5. In the **View** menu, select **Compliance rule violations**.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Compliance reports – system role (page description) on page 1074

Displaying risk indexes and entitlements of my system roles' members

For every system role that you are responsible for, you can see all the identities that have these system roles as primary or secondary assignments. You can also display the number of permissions assigned and the risk index.

To display members of a system role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose members you want to display.
4. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <system role name>** page (see Compliance reports – system role (page description) on page 1074).
5. In the **View** menu, select **Identities: Risk indexes and entitlements**.
6. (Optional) To display more information about an identity, perform the following actions:
   a. In the list, click an identity.
   b. In the dialog, click **Overview**.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Compliance reports – system role (page description) on page 1074

My system roles' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my system roles' attestation cases on page 440
- Displaying attestors of my system roles' pending attestation cases on page 442
- Approving and denying my system roles' attestation cases on page 443
- Sending reminders about my system roles' pending attestation cases on page 444

Displaying my system roles' attestation cases

You can see attestation cases that involve system roles for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <system role name>** page (see Attestation – System role (page description) on page 1069).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Attestation – System role (page description) on page 1069

Displaying attestors of my system roles' pending attestation cases

You can see identities that still have pending attestation cases from system roles for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Attestation – System role (page description) on page 1069

Approving and denying my system roles' attestation cases

You can grant or deny approval to attestation cases of system roles for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
6. Click **Approve**.
7. On the **Pending Attestations - <system role name>** page, perform one of the following actions:
    - Click ☑ (**Approve**) next to the attestation case you want to approve.
    - Click ☒ (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Attestation – System role (page description) on page 1069

Sending reminders about my system roles' pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

This opens an email template with the attestor's email address.

10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Attestation – System role (page description) on page 1069

Displaying my system roles' risk indexes

You can see risk indexes of system roles for which you are responsible.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a system role's risk index

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose risk index you want to display.
4. On the overview page, click **Risk**.

   This opens the **Risk - <system role name>** page (see Risk – System role (page description) on page 1071).
5. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Risk – System role (page description) on page 1071

My system roles' history

The Web Portal gives you the option of displaying the historical data of system roles for which you are responsible.

To do this, you have the following options:

Table 35: Historical data

View	Description
Events	This shows you all the events that affect the system role, either on a timeline or in a table (see Displaying my system roles' history on page 447).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only

View	Description
	see the initial and current status but you also see all the steps in between (see Displaying the status overview of my system roles on page 448).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my system roles on page 448).

Displaying my system roles' history

You can see all the events affecting system roles that you are responsible for, either on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <system role name>** page (see History – System role (page description) on page 1072).

   TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

   To zoom in or out, turn the mouse wheel.
5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:

- Click on the event in the timeline.
- In the table view, click the event and you will see the details in the details pane.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- History – System role (page description) on page 1072

Displaying the status overview of my system roles

You can see all the changes effecting system roles for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <system role name>** page (see History – System role (page description) on page 1072).
5. Click the **Status overview** tab.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- History – System role (page description) on page 1072

Comparing statuses of my system roles

You can compare the current status of a system role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since creation, deselect the check box next to **Display changed values only**.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- History – System role (page description) on page 1072

Displaying role memberships of my system roles' members

You can display the roles and organizations belonging to identities that are assigned system roles for which you are responsible. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a system role

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose members you want to know more about.
4. On the overview page, click **Usage**.

   This opens the **Usage - <system role name>** page (see Usage – System role (page description) on page 1074).
5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- My responsibilities (page description) on page 1014
- System roles (page description) on page 1061
- System role overview page (page description) on page 1063
- Usage – System role (page description) on page 1074

Managing my assignment resources

Use assignment resources to request hierarchical roles, such as departments or business roles and assign them to identities, devices, and workdesks. This means, for example, you can limit assignment resources to a certain business roles, which makes it unnecessary to select the business role additionally when you request an assignment resource. It is automatically a part of the assignment request.

For more information about assignment resources, see the *One Identity Manager Business Roles Administration Guide and One Identity Manager IT Shop Administration Guide*.

You can perform a variety of actions on the application roles that you manage and gather information about them.

Detailed information about this topic

- Displaying my assignment resources on page 451
- Displaying my assignment resource overviews on page 451
- Displaying and editing my assignment resource main data on page 452
- My assignment resources' attestations on page 452

Displaying my assignment resources

You can see all the assignment resources for which you are responsible.

To display assignment resources

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.

   This opens the **Assignment resources** page (see Assignment resources (page description) on page 1136) and displays all the assignment resources for which you are responsible.

Related topics

- My responsibilities (page description) on page 1014
- Assignment resources (page description) on page 1136

Displaying my assignment resource overviews

You can see all the relevant information about assignment resources that you are responsible for in the summarized form of an overview. The information is represented by shapes in a HyperView.

To display an assignment resource's overview

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <assignment resource name>** page (see Overview – Assignment resource (page description) on page 1138).

Related topics

- My responsibilities (page description) on page 1014
- Assignment resources (page description) on page 1136
- Assignment resource overview page (page description) on page 1137
- Overview – Assignment resource (page description) on page 1138

Displaying and editing my assignment resource main data

You can edit the main data of the assignment resources for which you are responsible.

To display and edit an assignment resource's main data

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <assignment resource name>**, make your changes in the respective fields (see Main data – Assignment resource (page description) on page 1138).
6. Click **Save**.

Related topics

- My responsibilities (page description) on page 1014
- Assignment resources (page description) on page 1136
- Assignment resource overview page (page description) on page 1137
- Main data – Assignment resource (page description) on page 1138

My assignment resources' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying my assignment resource pending attestation cases on page 453
- Displaying attestors of my assignment resource pending attestation cases on page 454
- Approving and denying my assignment resource attestation cases on page 455
- Sending reminders about my assignment resource pending attestation cases on page 456

Displaying my assignment resource pending attestation cases

You can see attestation cases that involve assignment resources for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <assignment resource name>** page (see Attestation - Assignment resource (page description) on page 1139).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview in shapes of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:

a. In the list, click the attestation case.

b. In the details pane, click the **Workflow** tab.

8. (Optional) To show previous attestation cases for the selected object, perform the following actions:

   a. In the list, click the attestation case.

   b. In the details pane, click the **History** tab.

   This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Assignment resources (page description) on page 1136
- Assignment resource overview page (page description) on page 1137
- Attestation - Assignment resource (page description) on page 1139

Displaying attestors of my assignment resource pending attestation cases

You can see identities that still have pending attestation cases from assignment resources for which you are responsible.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.

3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.

   On the **Devices** page, click the device whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- My responsibilities (page description) on page 1014
- Assignment resources (page description) on page 1136
- Assignment resource overview page (page description) on page 1137
- Attestation - Assignment resource (page description) on page 1139

Approving and denying my assignment resource attestation cases

You can grant or deny approval to attestation cases of assignment resources for which you are responsible.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to make an approval decision about.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Attestation - <assignment resource>** page, perform one of the following actions:
   - Click (**Approve**) next to the attestation case you want to approve.
   - Click (**Deny**) next to the attestation case you want to deny.

   TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).

8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. Click **Save**.

Related topics

- Attestation on page 153
- My responsibilities (page description) on page 1014
- Assignment resources (page description) on page 1136
- Assignment resource overview page (page description) on page 1137
- Attestation - Assignment resource (page description) on page 1139

Sending reminders about my assignment resource pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).

- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **My Responsibilities**.
2. On the **My Responsibilities** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

5. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- My responsibilities (page description) on page 1014
- Assignment resources (page description) on page 1136
- Assignment resource overview page (page description) on page 1137
- Attestation - Assignment resource (page description) on page 1139

Delegating tasks

You can temporarily delegate role memberships and responsibilities (and associated entitlements and duties) to other identities.
For example, if you go on vacation, you can hand over responsibility for a department and the associated tasks to a deputy.

Role memberships and responsibilities can also be delegated to you.

NOTE: In the Web Portal, a delegation is treated like a request.

Detailed information about this topic

- Displaying delegations on page 458
- Creating delegations on page 459
- Canceling delegations on page 460
- Deleting delegations on page 461
- Displaying delegation history on page 462
- My identities' delegations on page 306

Displaying delegations

You can see delegations created by you or by others for you.

To display delegations

1. In the menu bar, click **Responsibilities** > **Delegation**.
2. On the **Delegation** page, click **Delegation**.

   This opens the **Delegation** page (see Delegation (page description) on page 1170).
3. (Optional) To show more details about a delegation, perform one of the following actions:
   a. In the list, click the delegation whose details you want to show.
   b. In the details pane, click **Details**.

Related topics

- Deleting my identities' delegations on page 306
- Displaying identity delegations on page 648
- Delegating tasks (page description) on page 1170
- Delegation (page description) on page 1170

Creating delegations

You can delegate role memberships and responsibilities to other identities.

NOTE: You cannot edit a delegation afterward. If you want to make a change to the delegation, delete the it (see Deleting delegations on page 461) and create a new delegation.

To create a delegation

1. In the menu bar, click **Responsibilities** > **Delegation**.
2. On the **Delegation** page, click **Delegation**.
3. On the **Delegations** page, click **New delegation**.
4. In the **Delegation of role memberships and responsibilities** dialog, select the identity to which you want to delegate in the **Recipient** field.

   TIP: For a more detailed search for an identity, click **Assign** and select the appropriate identity in the **Recipient** dialog.
5. Click **Next**.
6. In the **Select roles** step, in the list, select the check boxes in front of the role memberships/responsibilities you want to delegate.
7. Click **Next**.
8. In the **Add additional information** set, configure the following settings:
   - **Valid from**: Specify from when the role/responsibility will be delegated.
   - **Valid until**: Specify until when the role/responsibility will be delegated.

- **Notify me if the recipient of the delegation makes a decision**: (Optional) Select the check box if you want to be notified when the recipient makes an approval decision about a delegated role/responsibility.
- **The recipient can delegate this role**: (Optional) Select the check box to specify that the recipient can delegate their delegated role/responsibility on to another identity.
- **Reason**: (Optional) In the dialog, enter a reason for the delegation.
- **Priority**: (Optional) In the menu, select a priority for the delegation.

9. Click **Save**.
10. In the Results step, click **Close**.

Related topics

- Adding delegations for my identities on page 307
- Adding delegations for identities on page 648
- Delegating tasks (page description) on page 1170
- Delegation (page description) on page 1170

Canceling delegations

You can cancel delegations that you have already set up.

NOTE: You can only cancel delegations as long they have the **Request** or **Approved** status. You can delete delegations with the **Assigned** status (see Deleting delegations on page 461).

To cancel a delegation

1. In the menu bar, click **Responsibilities** > **Delegation**.
2. On the **Delegation** page, click **Delegation**.
3. On the **Delegation** page, click the delegation in the list that you want to cancel.
4. In the details pane, click **Cancel request**.
5. Confirm the prompt with **Yes** in the dialog.

Related topics

- Canceling my identities' delegations on page 307
- Canceling identity delegations on page 649
- Delegating tasks (page description) on page 1170
- Delegation (page description) on page 1170

Deleting delegations

You can delete delegations that you created. That is, responsibilities that you have delegated to others become your responsibility again.

NOTE: You can only delete delegations as long as they have the **Assigned** status. You can cancel delegations that have the **Request** or **Approved** status (see Canceling delegations on page 460).

To delete a delegation

1. In the menu bar, click **Responsibilities** > **Delegation**.
2. On the **Delegation** page, click **Delegation**.
3. On the **Delegation**, click the delegation in the list that you want to delete.
4. In the details pane, click (**Delete**).
5. Confirm the prompt with **Yes** in the dialog.

To delete multiple delegations

1. In the menu bar, click **Responsibilities** > **Delegation**.
2. On the **Delegation** page, click **Delegation**.
3. On the **Delegation** page, click (**Select**) next to the delegations you want to delete.

   TIP: To select all the delegations shown, click (**Select all**).
4. Click **Actions** > **Delete delegation**.
5. Confirm the prompt with **Yes** in the dialog.

To delete all delegations

1. In the menu bar, click **Responsibilities** > **Delegation**.
2. On the **Delegation** page, click **Delegation**.
3. On the **Delegation** page, click **Actions** > **Delete all my delegations**.
4. Confirm the prompt with **Yes** in the dialog.

Related topics

- Deleting my identities' delegations on page 308
- Deleting identities' delegations on page 649
- Delegating tasks (page description) on page 1170
- Delegation (page description) on page 1170

Displaying delegation history

You can display past delegations created by you or by others for you.

To show delegation history

1. In the menu bar, click **Responsibilities** > **Delegation**.
2. On the **Delegation** page, click **Delegation history**.

   This opens the **Delegation History** page (see Delegation history (page description) on page 1172).
3. (Optional) To limit delegations to display to a specific time period, make the following settings:
   - **Valid from**: All delegations that are valid as from this time on or from a time point within this period are taken into account.
   - **Valid until**: All delegations that are valid up to this time or up to a time point within this period are taken into account.
4. (Optional) To display only delegations about a specific identity, perform the following actions:
   a. Click **Advanced search**.
   b. Click **Assign** next to the **Delegator** field.
   c. In the **Employee** dialog, click the identity that issued the delegation.
5. (Optional) To display only delegations issued to a specific identity, take the following actions:
   a. Click **Advanced search**.
   b. Click **Assign** next to **Delegation recipient**.
   c. In the **Employee** dialog, click the identity to whom the delegation was issued.
6. (Optional) To display delegations that are not in effect, take the following actions:
   a. Click **Advanced search**.
   b. Select the **Show never assigned delegations** check box.
7. Click **Search**.
8. (Optional) To display details of a delegation, click it in the list.

   For each delegation, you can obtain more information about the delegation in the details pane on the **Information**, **Workflow**, **Compliance**, and **Permissions** tabs.

Examples

You want to display all delegations that are valid as of January 1, 2019:

1. Clear all the date fields except for the first one next to **Valid from**.
2. In the field next to **Valid from**, select the date **01/01/2019**.
3. Click **Search**.

You want to display all delegations that are valid as of January 1, 2019 until February 1, 2019:

1. Clear the all date fields apart from the one next to **Valid from** and the first **Valid until**.
2. In the field next to **Valid from**, select the date **01/01/2019**.
3. In the field next to **Valid until**, select the date **02/01/2019**.
4. Click **Search**.

You want to show all delegations with a valid from date between 01/01/2019 and 01/03/2019:

1. Clear all the date fields except for the first and second ones next to **Valid from**.
2. In the first field next to **Valid from**, select the date **01/01/2019**.
3. In the second field next to **Valid from**, select the date **01/03/2019**.
4. Click **Search**.

Related topics

- Delegating tasks (page description) on page 1170
- Delegation history (page description) on page 1172

Ownerships

You can assign business objects to owners or assume ownership of them.

Detailed information about this topic

- Assigning owners to system entitlements on page 464
- Assigning owners to devices on page 464
- Claiming ownership of Active Directory groups on page 465

Assigning owners to system entitlements

You can specify who is responsible for a system entitlement. To do this, you define a product owner for the service item that is assigned to the system entitlement.

To assign system entitlements to an owner

1. In the menu bar, click **Responsibilities** > **Ownerships**.
2. On the **Ownerships** page, click **Assign Owner**.
3. On the **Assign Ownership** page, click **System entitlement**.
4. In the **Assign an owner to a system entitlement** dialog, click **Assign** next to **Device**.
5. In the **System entitlement** dialog, click the system entitlement to which you want to assign an owner.
6. In the **Assign an owner to a system entitlement** dialog, click **Next**.
7. In the **Specify the new owner** step, perform one of the following actions:
   - To allow owners to be determined automatically, click **Select one of the calculated possible owners** and then select the identity in the menu.
   - To set a specific identity as the owner, click **Select another owner**, and then click **Assign**. Now click the identity you want to specify as the owner.
8. Click **Next**.
9. In the **Results** step, click **Close**.

   In the context of an attestation, the selected owner can confirm that this assignment is correct (see Pending attestations on page 177).

Related topics

- Assigning owners to devices on page 464
- Claiming ownership of Active Directory groups on page 465
- Ownerships (page description) on page 1174
- Assigning owners (page description) on page 1174

Assigning owners to devices

You can specify who is responsible for a device. To do this, you define a product owner for the service item that is assigned to the device.

To assign an owner to a device

1. In the menu bar, click **Responsibilities** > **Ownerships**.
2. On the **Ownerships** page, click **Assign Owner**.
3. On the **Assign Ownership** page, click **Device**.
4. In the **Assign an owner to a device** dialog, click **Assign** next to **System entitlementDevice**.
5. In the **Device** dialog, click the device to which you want to assign an owner.
6. In the **Assign an owner to a device** dialog, click **Next**.
7. In the **Specify the new owner** step, perform one of the following actions:
    - To allow owners to be determined automatically, click **Select one of the calculated possible owners** and then select the identity in the menu.
    - To set a specific identity as the owner, click **Select another owner**, and then click **Assign**. Now click the identity you want to specify as the owner.
8. Click **Next**.
9. In the **Results** step, click **Close**.

    In the context of an attestation, the selected owner can confirm that this assignment is correct (see Pending attestations on page 177).

Related topics

- Assigning owners to system entitlements on page 464
- Claiming ownership of Active Directory groups on page 465
- Ownerships (page description) on page 1174
- Assigning owners (page description) on page 1174

Claiming ownership of Active Directory groups

You can claim ownership of Active Directory groups if they do not have an owner.

If you claim ownership for a group, you are accountable for the interests of that group. For example, you decide about memberships within your group.

To claim ownership of a group

1. In the menu bar, click **Responsibilities** > **Ownerships**.
2. On the **Ownerships** page, click **Claim Ownership**.
3. On the **Claim Ownership** page, click **Assign**.

4. In the **Select a group** dialog box, click the Active Directory group for which you want to claim ownership.
5. On the **Claim Ownership** page, click **Claim Ownership**.

Related topics

- Assigning owners to system entitlements on page 464
- Assigning owners to devices on page 464

Auditing

Auditing describes how an aspect of a company is assessed. Quality assurance is also plays an important part in auditing. An audit is a systematic, independent, and documented examination, which assesses quality-related actions and evaluates them based on the planned requirements and targets. To successfully complete an audit there must be certain features available and specific requirements must be fulfilled.

Detailed information about this topic

- Auditing departments on page 466
- Auditing application roles on page 478
- Auditing devices on page 489
- Auditing business roles on page 493
- Auditing identities on page 505
- Auditing cost centers on page 517
- Auditing multi-request resources on page 529
- Auditing multi requestable/unsubscribable resources on page 534
- Auditing resources on page 540
- Auditing software on page 546
- Auditing locations on page 552
- Auditing system roles on page 564
- Auditing system entitlements on page 576
- Auditing assignment resources on page 585

Auditing departments

You can gather various information about departments.

Detailed information about this topic

- Displaying all departments on page 467
- Displaying department overviews on page 467
- Displaying department main data on page 468
- Displaying department memberships on page 469
- Displaying department entitlements on page 469
- Department attestations on page 470
- Department compliance on page 473
- Displaying department risk indexes on page 474
- Department history on page 474
- Displaying role memberships of department members on page 478

Displaying all departments

You can see all the departments.

To display departments

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.

   This opens the **Auditing - Departments** page (see Auditing – Departments (page description) on page 1176) and displays all the departments.
3. (Optional) To display only departments for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176

Displaying department overviews

You can see all relevant information about departments summarized in an overview. The information is represented by shapes in a HyperView.

To display a department's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <department name>** page (see Overview – Department (page description) on page 1178).

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- Overview – Department (page description) on page 1178

Displaying department main data

You can see departments' main data.

To display a department's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <department name>** page displays the main data (see Main data – Department (page description) on page 1178).

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- Main data – Department (page description) on page 1178

Displaying department memberships

You can see identities that have departments assigned to them.

To display identities that are assigned a department

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <department name>** page (see Memberships – Department (page description) on page 1179).

Related topics

- My responsibilities (page description) on page 1014
- Departments (page description) on page 1076
- Department overview page (page description) on page 1077
- Memberships – Department (page description) on page 1080

Displaying department entitlements

You can see entitlements assigned to departments. You can also display the reason why departments have certain entitlements (entitlement origin).

To display a department's entitlements

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <department name>** page (see Entitlements – Department (page description) on page 1180).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to

Analysis for.

This displays more information about the entitlement's assignment.

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- Entitlements – Department (page description) on page 1180

Department attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying department attestation cases on page 470
- Displaying attestors of department pending attestation cases on page 472

Displaying department attestation cases

You can see the departments' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <department name>** page (see Attestation – Department (page description) on page 1181).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- Attestation – Department (page description) on page 1181

Displaying attestors of department pending attestation cases

You can see identities that still have to approve department attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- Attestation – Department (page description) on page 1181

Department compliance

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying department rule violations on page 473

Displaying department rule violations

You can see department rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose rule violations you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Compliance**.

   This opens the **Compliance - <department name>** page (see Compliance – Department (page description) on page 1182).

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- Compliance – Department (page description) on page 1182

Displaying department risk indexes

You can see department risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a department's risk index

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose risk index you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Risk**.

   This opens the **Risk - <department name>** page (see Risk – Department (page description) on page 1183).
6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- Risk – Department (page description) on page 1183

Department history

The Web Portal offers you the option to display departments' historical data.

To do this, you have the following options:

Table 36: Historical data

View	Description
Events	This shows you all the events that affect the department, either on a timeline or in a table (see Displaying my department history on page 238).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my departments on page 239).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my departments on page 239).

Displaying department history

You can select to display all events involving departments on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose history you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <department name>** page (see History – Department (page description) on page 1183).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.

6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.

- **Properties**: Only show events on the timeline with the selected properties.
- **Display**: Only show events on the timeline that match the search.
- **Object**: Only show events on the timeline about the selected object.

7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- History – Department (page description) on page 1183

Displaying the status overview of departments

You can see all the changes that affect departments. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose status overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <department name>** page (see History – Department (page description) on page 1183).
6. Click the **Status overview** tab.

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- History – Department (page description) on page 1183

Comparing statuses of departments

You can compare the current state of a department with its state at another time.

To compare states

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose state you want to compare.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.
6. On the **History - <department name>** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose state you want to compare.
4. On the overview page, click **History**.
5. On the **History - <department name>** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- History – Department (page description) on page 1183

Displaying role memberships of department members

You can see which roles and organizations belong to identities that are assigned departments. . Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a department

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Departments**.
3. On the **Auditing - Departments** page, click the department whose members you want to know more about.
4. In the details pane, click **Show details**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <department name>** page (see Usage – Department (page description) on page 1185).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Departments (page description) on page 1176
- Auditing - Roles and permissions: department (page description) on page 1177
- Usage – Department (page description) on page 1185

Auditing application roles

Use application roles to assign entitlement profiles to identities that match their tasks and functions. One Identity Manager already supplies a number of default application roles.

You can gather various information about application roles.

Detailed information about this topic

- Displaying all application roles on page 479
- Displaying application role overviews on page 479
- Displaying application role main data on page 480
- Displaying memberships in application roles on page 481
- Displaying application role entitlements on page 481
- Application role attestations on page 482
- Application role history on page 485
- Displaying role memberships of application role members on page 488

Displaying all application roles

You can see all the application roles.

To display application roles

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.

   This opens the **Auditing - Application Roles** page (see Auditing – Application roles (page description) on page 1186) and displays all the application roles.
3. (Optional) To display only application roles for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186

Displaying application role overviews

You can see all relevant information about application roles summarized in an overview. The information is represented by shapes in a HyperView.

To display an application role's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <application role name>** page (see Overview – Application role (page description) on page 1188).

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- Overview – Application role (page description) on page 1188

Displaying application role main data

You can see application roles' main data.

To display an application role's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <application role name>** page displays the main data (see Main data - Application role (page description) on page 1188).

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- Main data - Application role (page description) on page 1188

Displaying memberships in application roles

You can see identities that have application roles assigned to them.

To display identities that are assigned an application role

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <application role name>** page (see Memberships – Application role (page description) on page 1189).

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- Memberships – Application role (page description) on page 1189

Displaying application role entitlements

You can see entitlements assigned to application roles. You can also display the reason why application roles have certain entitlements (entitlement origin).

To display an application role's entitlements

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <application role name>** page (see Entitlements – Application role (page description) on page 1190).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to

Analysis for.

This displays more information about the entitlement's assignment.

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- Entitlements – Application role (page description) on page 1190

Application role attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying application role pending attestation cases on page 482
- Displaying attestors of application role pending attestation cases on page 484

Displaying application role pending attestation cases

You can see the application roles' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <application role name>** page (see Attestation – Application role (page description) on page 1190).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- Attestation – Application role (page description) on page 1190

Displaying attestors of application role pending attestation cases

You can see identities that still have to approve application role attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <application role name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <application role name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- Attestation – Application role (page description) on page 1190

Application role history

The Web Portal offers you the option to display application roles' historical data.

To do this, you have the following options:

Table 37: Historical data

View	Description
Events	This shows you all the events that affect the application role, either on a timeline or in a table (see Displaying my application roles' history on page 258).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my application roles on page 259).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my application roles on page 260).

Displaying application role history

You can select to display all events involving application roles on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose history you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <application role name>** page (see History – Application role (page description) on page 1192).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.
6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:

- **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
- **Change type**: Only show events on the timeline with the selected change type.
- **Date**: Only show events on the timeline that took place in the given period.
- **Properties**: Only show events on the timeline with the selected properties.
- **Display**: Only show events on the timeline that match the search.
- **Object**: Only show events on the timeline about the selected object.

7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- History – Application role (page description) on page 1192

Displaying the status overview of application roles

You can see all the changes that affect application roles. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose status overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <application role name>** page (see History – Application role (page description) on page 1192).
6. Click the **Status overview** tab.

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- History – Application role (page description) on page 1192

Comparing statuses of application roles

You can compare the current state of an application role with its state at another time.

To compare states

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose state you want to compare.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.
6. On the **History - <application role name>** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application roles** page, click the application role whose state you want to compare.
4. On the overview page, click **History**.
5. On the **History - <application role name>** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- History – Application role (page description) on page 1192

Displaying role memberships of application role members

. You can see which roles and organizations belong to identities that are assigned application roles. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of an application role

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Application roles**.
3. On the **Auditing - Application Roles** page, click the application role whose members you want to know more about.
4. In the details pane, click **Show details**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <application role name>** page (see Usage – Application role (page description) on page 1194).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Application roles (page description) on page 1186
- Auditing - Roles and entitlements: application role (page description) on page 1187
- Usage – Application role (page description) on page 1194

Auditing devices

You can gather various information about devices.

Detailed information about this topic

- Displaying devices on page 489
- Displaying device overviews on page 489
- Displaying device main data on page 490
- Device attestations on page 491

Displaying devices

You can see all the devices.

To display devices

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Devices**.

   This opens the **Auditing - Devices** page (see Auditing – Device (page description) on page 1195) and displays all the devices.
3. (Optional) To display only devices for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Device (page description) on page 1195

Displaying device overviews

You can see all relevant information about devices summarized in an overview. The information is represented by shapes in a HyperView.

To display a device's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Devices**.
3. On the **Auditing - Device** page, click the device whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <device name>** page (see Overview – Device (page description) on page 1196).

Related topics

- Auditing (page description) on page 1175
- Auditing – Device (page description) on page 1195
- Auditing - Roles and entitlements: device (page description) on page 1195
- Overview – Device (page description) on page 1196

Displaying device main data

You can see devices' main data.

To display a device's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Devices**.
3. On the **Auditing - Device** page, click the device whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <device name>** page displays the main data (see Main data – Device (page description) on page 1196).

Related topics

- Auditing (page description) on page 1175
- Auditing – Device (page description) on page 1195
- Auditing - Roles and entitlements: device (page description) on page 1195
- Main data – Device (page description) on page 1196

Device attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying device attestation cases on page 491
- Displaying attestors of pending attestation cases for devices on page 492

Displaying device attestation cases

You can see the devices' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Devices**.
3. On the **Auditing - Device** page, click the device whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <device name>** page (see Attestations – Device (page description) on page 1199).
6. (Optional) Click on a tab to display the respective attestation cases.

7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – Device (page description) on page 1195
- Auditing - Roles and entitlements: device (page description) on page 1195
- Attestations – Device (page description) on page 1199

Displaying attestors of pending attestation cases for devices

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Devices**.
3. In the details pane, click **Show details**.
4. On the overview page, click **Attestation**.
5. In the list, click the (pending) attestation case that has attestors you want to display.
6. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Devices**.
3. In the details pane, click **Show details**.
4. On the overview page, click **Attestation**.
5. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – Device (page description) on page 1195
- Auditing - Roles and entitlements: device (page description) on page 1195
- Attestations – Device (page description) on page 1199

Auditing business roles

You can gather various information about business roles.

Detailed information about this topic

- Displaying all business roles on page 493
- Displaying business role overviews on page 494
- Displaying business role main data on page 495
- Displaying memberships in business roles on page 495
- Displaying business role entitlements on page 496
- Business role attestations on page 496
- Business role compliance on page 499
- Displaying business role risk indexes on page 500
- Business role history on page 501
- Displaying role memberships of business role members on page 504

Displaying all business roles

You can see all the business roles.

To display business roles

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.

   This opens the **Auditing - Business Roles** page (see Auditing – Business roles (page description) on page 1200) and displays all the business roles.
3. (Optional) To display only business roles for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200

Displaying business role overviews

You can see all relevant information about business roles summarized in an overview. The information is represented by shapes in a HyperView.

To display a business role's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <business role name>** page (see Overview – Business role (page description) on page 1203).

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- Overview – Business role (page description) on page 1203

Displaying business role main data

You can see business roles' main data.

To display a business role's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <business role name>** page displays the main data (see Main data – Business role (page description) on page 1203).

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- Main data – Business role (page description) on page 1203

Displaying memberships in business roles

You can see identities that have business roles assigned to them.

To display identities that are assigned a business role

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <business role name>** page (see Memberships – Business role (page description) on page 1204).

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200

- Auditing - Roles and entitlements: business role (page description) on page 1201
- Memberships – Business role (page description) on page 1204

Displaying business role entitlements

You can see entitlements assigned to business roles. You can also display the reason why business roles have certain entitlements (entitlement origin).

To display a business role's entitlements

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <business role name>** page (see Entitlements – Business role (page description) on page 1205).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- Entitlements – Business role (page description) on page 1205

Business role attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying business role attestation cases on page 497
- Displaying attestors of business role pending attestation cases on page 498

Displaying business role attestation cases

You can see the business roles' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <business role name>** page (see Attestation – Business role (page description) on page 1205).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.

8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- Attestation – Business role (page description) on page 1205

Displaying attestors of business role pending attestation cases

You can see identities that still have to approve business role attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- Attestation – Business role (page description) on page 1205

Business role compliance

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying business role rule violations on page 500

Displaying business role rule violations

You can see business role rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose rule violations you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Compliance**.

   This opens the **Compliance - <business role name>** page (see Compliance – Business role (page description) on page 1206).

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- Compliance – Business role (page description) on page 1206

Displaying business role risk indexes

You can see business role risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a business role's risk index

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose risk index you want to display.
4. In the details pane, click **Show details**.

5. On the overview page, click **Risk**.

   This opens the **Risk - <business role name>** page (see Risk – Business role (page description) on page 1207).
6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- Risk – Business role (page description) on page 1207

Business role history

The Web Portal offers you the option to display business roles' historical data.

To do this, you have the following options:

Table 38: Historical data

View	Description
Events	This shows you all the events that affect the business role, either on a timeline or in a table (see Displaying my business roles' history on page 290).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my business roles on page 291).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my business roles on page 291).

Displaying business role history

You can select to display all events involving business roles on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose history you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <business role name>** page (see History – Business role (page description) on page 1208).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.
6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- History – Business role (page description) on page 1208

Displaying the status overview of business roles

You can see all the changes that affect business roles. You can also display how long each change was valid for. Use the status overview to track when changes were made and by

whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose status overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <business role name>** page (see History – Business role (page description) on page 1208).
6. Click the **Status overview** tab.

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- History – Business role (page description) on page 1208

Comparing statuses of business roles

You can compare the current state of a business role with its state at another time.

To compare states

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose state you want to compare.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.
6. On the **History - <business role name>** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose state you want to compare.
4. On the overview page, click **History**.
5. On the **History - <business role name>** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- History – Business role (page description) on page 1208

Displaying role memberships of business role members

You can see which roles and organizations belong to identities that are assigned business roles. . Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

| MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a business role

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Business Roles**.
3. On the **Auditing - Business roles** page, click the business role whose members you want to know more about.
4. In the details pane, click **Show details**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <business role name>** page (see Usage – Business role (page description) on page 1210).

6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Business roles (page description) on page 1200
- Auditing - Roles and entitlements: business role (page description) on page 1201
- Usage – Business role (page description) on page 1210

Auditing identities

You can gather various information about identities.

Detailed information about this topic

- Displaying all identities on page 505
- Displaying identity overviews on page 506
- Displaying identity main data on page 506
- Displaying identity requests on page 507
- Displaying identity approvals on page 507
- Displaying identity entitlements on page 508
- Displaying identity responsibilities on page 509
- Identity attestations on page 510
- Identity compliance on page 512
- Displaying identity risk indexes on page 514
- Identity history on page 514

Displaying all identities

You can see all the identities.

To display identities

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.

This opens the **Auditing - Identity Details** page (see Auditing – Identity details (page description) on page 1211) and displays all the identities.

Related topics

- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211

Displaying identity overviews

You can see all relevant information about identities summarized in an overview. For example, this information includes identities, requests, rule violations, user accounts, subidentities, assigned permissions, and memberships. The information is represented by shapes in a HyperView.

To display an identity's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <identity's name>** page (see Overview – Identity (page description) on page 1213).

Related topics

- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Overview – Identity (page description) on page 1213

Displaying identity main data

You can see identities' main data.

To display an identity's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose main data you want to display.

4. On the overview page, click **Main data**.
5. This opens the **Main data - <identity name>** page displays the main data (see Main data – Identity (page description) on page 1213).

Related topics

- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Main data – Identity (page description) on page 1213

Displaying identity requests

You can display requests made by identities. All requests that identities have made themselves or that have been made for them (for example, by a manager) are displayed.

To display requests of an identity

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose requests you want to display.
4. On the overview page, click **Requests**.

   This opens the**Requests- <name of identity>** page (see Requests - Identities ((page description)) on page 1215).
5. (Optional) Click **Advanced Search** to control which requests are displayed (see Requests - Identities ((page description)) on page 1215). For example, you can display only pending (not yet assigned) requests.

Related topics

- Displaying request history on page 128
- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Requests - Identities ((page description)) on page 1215

Displaying identity approvals

You can display the following approval-related information for identities:

- All approval processes for product requests that the identity was involved in and their approval decisions.
- All rule violations dealt with by the identity
- All approval processes for attestation that the identity was involved in and their approval decisions.
- All policy violations dealt with by the selected identity

To display an identity's approvals

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose approvals you want to display.
4. On the overview page, click **Approvals**.

   This opens the **Approvals - <identity name>** page and shows all the approval processes for product requests that the identity was involved in and their approval decisions (see Approvals – Identity (page description) on page 1217).
5. (Optional) To control which requests are displayed, click **Advanced search** (see Approvals – Identity (page description) on page 1217). For example, you can display only pending (not yet assigned) requests.
6. (Optional) Perform one of the following actions:
   - To display all rule violations that have been handled by the identity, click the **Exception approvals** tab.
   - To display all attestation approval processes in which the identity was involved and their decisions, click the **Attestation** tab.
   - To display all policy violations edited by the selected identity, click the **Policy Violations** tab.

Related topics

- Displaying approvals on page 132
- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Approvals – Identity (page description) on page 1217

Displaying identity entitlements

You can see entitlements assigned to identities. You can also display the reason why identities have certain entitlements (entitlement origin).

To display an identity's entitlements

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <identity's name>** page (see Entitlements – Identity (page description) on page 1221).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Entitlements – Identity (page description) on page 1221

Displaying identity responsibilities

You can display all the objects for which the identities are responsibility.

To display an identity's responsibilities

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose responsibilities you want to display.
4. On the overview page, click **Responsibilities**.

   This **Auditing - <name of identity>** page (see Responsibilities - Identity (page description) on page 1222).
5. In the **Object type** drop-down, select which of the identity's objects you want to display (for example, departments).
6. (Optional) To display an object's details, perform the following actions:

    a. In the list, click on the object.
    b. In the details pane, click **Show details**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Responsibilities - Identity (page description) on page 1222

Identity attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

Displaying attestation cases of identities

You can see the identities' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.

3. On the **Auditing - Identity Details** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <identity's name>** page (see Attestations – Identity (page description) on page 1222).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Attestation on page 153
- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Attestations – Identity (page description) on page 1222

Displaying attestors of identity pending attestation cases

You can see identities that still have to approve identities attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity's name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity's name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestation on page 153
- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Attestations – Identity (page description) on page 1222

Identity compliance

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying identities' rule violations on page 513

Displaying identities' rule violations

You can display the rule violations of identities.

To display an identity's rule violations

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose rule violations you want to display.
4. On the **Auditing - identity's name>** page, click **Rule Violations**.

   This opens the **Rule Violations - <identity's name>** page (see Rule violations – Identity (page description) on page 1224).

Related topics

- Managing rule violations on page 201
- Displaying compliance rules and rule violations on page 213
- Displaying rule violations of identities with critical SAP functions on page 217
- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Rule violations – Identity (page description) on page 1224

Displaying identity risk indexes

You can see identities risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display an identity's risk index

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose risk index you want to display.
4. On the overview page, click **Risk**.

   This opens the **Risk - <identity's name>** page (see Risk – Identity (page description) on page 1225).
5. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- Risk – Identity (page description) on page 1225

Identity history

The Web Portal offers you the option to display identities' historical data.

To do this, you have the following options:

Table 39: Historical data

View	Description
Events	This shows you all the events that affect the identity, either on a timeline or in a table (see Displaying my identity history on page 315).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my identities on

View	Description
	page 316).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my identities on page 317).

Displaying identity history

You can select to display all events involving identities on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <identity's name>** page (see History – Identity (page description) on page 1226).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.
5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- History – Identity (page description) on page 1226

Displaying the status overview of identities

You can see all the changes that affect identities. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <identity's name>** page (see History – Identity (page description) on page 1226).
5. Click the **Status overview** tab.

Related topics

- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- History – Identity (page description) on page 1226

Comparing statuses of identities

You can compare the current state of an identity with its state at another time.

To compare states

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose state you want to compare.
4. On the overview page, click **History**.

5. On the **History - <identity name>** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Identities**.
3. On the **Auditing - Identity Details** page, click the identity whose history you want to display.
4. On the overview page, click **History**.
5. On the **History - <identity name>** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Identity details (page description) on page 1211
- Auditing – Identity (page description) on page 1211
- History – Identity (page description) on page 1226

Auditing cost centers

You can gather various information about cost centers.

Detailed information about this topic

- Displaying all cost centers on page 518
- Displaying cost center overviews on page 518
- Displaying cost center main data on page 519
- Displaying memberships in cost centers on page 519
- Displaying cost center entitlements on page 520
- Cost center attestations on page 521
- Cost center compliance on page 523

- Displaying cost center risk indexes on page 524
- Cost center history on page 525
- Displaying role memberships of cost center members on page 528

Displaying all cost centers

You can see all the cost centers.

To display cost centers

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.

   This opens the **Auditing - Cost Centers** page (see Auditing – Cost center (page description) on page 1228) and displays all the cost centers.
3. (Optional) To display only cost centers for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228

Displaying cost center overviews

You can see all relevant information about cost centers summarized in an overview. The information is represented by shapes in a HyperView.

To display a cost center's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <cost center name>** page (see Overview – Cost center (page description) on page 1231).

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- Overview – Cost center (page description) on page 1231

Displaying cost center main data

You can see cost centers' main data.

To display a cost center's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <cost center name>** page displays the main data (see Main data – Cost center (page description) on page 1231).

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- Main data – Cost center (page description) on page 1231

Displaying memberships in cost centers

You can see identities that have cost centers assigned to them.

To display identities that are assigned a cost center

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

This opens the **Memberships - <cost center name>** page (see Memberships – Cost center (page description) on page 1232).

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- Memberships – Cost center (page description) on page 1232

Displaying cost center entitlements

You can see entitlements assigned to cost centers. You can also display the reason why cost centers have certain entitlements (entitlement origin).

To display a cost center's entitlements

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <cost center name>** page (see Entitlements – Cost center (page description) on page 1232).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- Entitlements – Cost center (page description) on page 1232

Cost center attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying cost center attestation cases on page 521
- Displaying attestors of cost center pending attestation cases on page 522

Displaying cost center attestation cases

You can see the cost centers' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <cost center name>** page (see Attestation – Cost center (page description) on page 1233).
6. (Optional) Click on a tab to display the respective attestation cases.

7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
    a. In the list, click an attestation case.
    b. In the details pane, click **Show details**.
    c. In the **Attested object** dialog, select an object in the **Object** menu.

       This shows information about the object.
    d. (Optional) Click **View current state of the object**

       This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
    a. In the list, click an attestation case.
    b. In the details pane, click the **History** tab.

       This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- Attestation – Cost center (page description) on page 1233

Displaying attestors of cost center pending attestation cases

You can see identities that still have to approve cost center attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

6. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- Attestation – Cost center (page description) on page 1233

Cost center compliance

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.

- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity's Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying cost center rule violations on page 524

Displaying cost center rule violations

You can see cost center rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose rule violations you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Compliance**.

   This opens the **Compliance - <cost center name>** page (see Compliance – Cost center (page description) on page 1234).

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- Compliance – Cost center (page description) on page 1234

Displaying cost center risk indexes

You can see cost center risk indexes.

> NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a cost center's risk index

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose risk index you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Risk**.

   This opens the **Risk - <cost center name>** page (see Risk – Cost center (page description) on page 1235).
6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- Risk – Cost center (page description) on page 1235

Cost center history

The Web Portal offers you the option to display cost centers' historical data.

To do this, you have the following options:

Table 40: Historical data

View	Description
Events	This shows you all the events that affect the cost center, either on a timeline or in a table (see Displaying my cost center history on page 335).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my cost centers on page 336).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my cost centers on page 337).

Displaying cost center history

You can select to display all events involving cost centers on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose history you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <cost center name>** page (see History – Cost center (page description) on page 1236).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.
6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- History – Cost center (page description) on page 1236

Displaying the status overview of cost centers

You can see all the changes that affect cost centers. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose status overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <cost center name>** page (see History – Cost center (page description) on page 1236).
6. Click the **Status overview** tab.

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- History – Cost center (page description) on page 1236

Comparing statuses of cost centers

You can compare the current state of a cost center with its state at another time.

To compare states

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose state you want to compare.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.
6. On the **History - <cost center name>** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.

8. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost centers** page, click the cost center whose state you want to compare.
4. On the overview page, click **History**.
5. On the **History - <cost center name>** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- History – Cost center (page description) on page 1236

Displaying role memberships of cost center members

You can see which roles and organizations belong to identities that are assigned cost centers. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a cost center

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Cost centers**.
3. On the **Auditing - Cost Centers** page, click the cost center whose members you want to know more about.
4. In the details pane, click **Show details**.
5. On the overview page, click **Usage**.

This opens the **Usage - <cost center name>** page (see Usage – Cost center (page description) on page 1238).

6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Cost center (page description) on page 1228
- Auditing - Roles and entitlements: cost center (page description) on page 1229
- Usage – Cost center (page description) on page 1238

Auditing multi-request resources

Multi-request resources are resources that an identity can request multiple times. Requests are automatically unsubscribed after approval. The resources are not explicitly assigned to the identity. Examples are consumables, such as pens or printer paper.

You can gather various information about multi-request resources.

Detailed information about this topic

- Displaying multi-request resources on page 529
- Displaying multi-request resource overviews on page 530
- Displaying multi-request resource main data on page 530
- Multi-request resource attestations on page 531

Displaying multi-request resources

You can see all the multi-request resources.

To display multi-request resources

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multiple requestable resources**.

   This opens the **Auditing - Multi-request Resources** page (see Auditing – Multi-request resources (page description) on page 1238) and displays all the multi-request resources.

3. (Optional) To display only multi-request resources for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi-request resources (page description) on page 1238

Displaying multi-request resource overviews

You can see all relevant information about multi-request resources summarized in an overview. The information is represented by shapes in a HyperView.

To display a multi-request resource's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multiple requestable resources**.
3. On the **Auditing - Multi-request resources** page, click the multi-request resource whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <multi-request resource name>** page (see Overview – Multi-request resource (page description) on page 1240).

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi-request resources (page description) on page 1238
- Auditing - Roles and entitlements: multi-request resource (page description) on page 1239
- Overview – Multi-request resource (page description) on page 1240

Displaying multi-request resource main data

You can see multi-request resources' main data

To display a multi-request resource's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multiple requestable resources**.
3. On the **Auditing - Multi-request resources** page, click the multi-request resource whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <multi-request resource name>** page displays the main data (see Main data – Multi-request resource (page description) on page 1240).

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi-request resources (page description) on page 1238
- Auditing - Roles and entitlements: multi-request resource (page description) on page 1239
- Main data – Multi-request resource (page description) on page 1240

Multi-request resource attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying multi-request resource attestation cases on page 532
- Displaying attestors of multi-request resource pending attestation cases on page 533

Displaying multi-request resource attestation cases

You can see the multi-request resource attestation cases

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multiple requestable resources**.
3. On the **Auditing - Multi-request resources** page, click the multi-request resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <multi-request resource name>** page (see Attestation – Multi-request resource (page description) on page 1241).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   1. In the list, click an attestation case.
   2. In the details pane, click **Show details**.
   3. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   4. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   1. In the list, click the attestation case.
   2. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   1. In the list, click an attestation case.
   2. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi-request resources (page description) on page 1238

- Auditing - Roles and entitlements: multi-request resource (page description) on page 1239
- Attestation – Multi-request resource (page description) on page 1241

Displaying attestors of multi-request resource pending attestation cases

You can see identities that still have to approve multi-request resource attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multiple requestable resources**.
3. On the **Auditing - Multi-request resources** page, click the multi-request resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multiple requestable resources**.
3. On the **Auditing - Multi-request resources** page, click the multi-request resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi-request resources (page description) on page 1238

- Auditing - Roles and entitlements: multi-request resource (page description) on page 1239
- Attestation – Multi-request resource (page description) on page 1241

Auditing multi requestable/unsubscribable resources

Multi requestable/unsubscribable resources are resources that an identity can request multiple times, but that must be explicitly returned when they are no longer needed. The resources are assigned to identities after approval has been granted and they remain assigned until the request is canceled.

You can gather various information about multi requestable/unsubscribable resources.

Detailed information about this topic

Displaying all multi requestable/unsubscribable resources

You can see all the multi requestable/unsubscribable resources.

To display multi requestable/unsubscribable resources

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multi requestable/unsubscribable resources**.

   This opens the **Auditing - Multi requestable/unsubscribable Resources** page (see Auditing – Multi requestable/unsubscribable resources (page description) on page 1243) and displays all the multi requestable/unsubscribable resources.
3. (Optional) To display only multi requestable/unsubscribable resources for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi requestable/unsubscribable resources (page description) on page 1243

Displaying multi requestable/unsubscribable resource overviews

You can see all relevant information about multi requestable/unsubscribable resources summarized in an overview. The information is represented by shapes in a HyperView.

To display a multi requestable/unsubscribable resource's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multi requestable/unsubscribable resources**.
3. On the **Auditing - Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <multi requestable/unsubscribable resource name>** page (see Overview – Multi requestable/unsubscribable resource (page description) on page 1245).

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi requestable/unsubscribable resources (page description) on page 1243
- Auditing - Roles and entitlements: multi requestable/unsubscribable resource (page description) on page 1244
- Overview – Multi requestable/unsubscribable resource (page description) on page 1245

Displaying multi requestable/unsubscribable resource main data

You can see multi requestable/unsubscribable resources' main data.

To display a multi requestable/unsubscribable resource's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multi requestable/unsubscribable resources**.
3. On the **Auditing - Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <multi requestable/unsubscribable resource name>** page displays the main data (see Main data – Multi requestable/unsubscribable resource (page description) on page 1245).

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi requestable/unsubscribable resources (page description) on page 1243
- Auditing - Roles and entitlements: multi requestable/unsubscribable resource (page description) on page 1244
- Main data – Multi requestable/unsubscribable resource (page description) on page 1245

Displaying memberships in multi requestable/unsubscribable resources

You can see identities that have multi requestable/unsubscribable resources assigned to them.

To display identities that are assigned a multi requestable/unsubscribable resource

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multi requestable/unsubscribable resources**.
3. On the **Auditing - Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <multi requestable/unsubscribable resource name>** page (see Memberships – Multi requestable/unsubscribable resource (page description) on page 1246).

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi requestable/unsubscribable resources (page description) on page 1243
- Auditing - Roles and entitlements: multi requestable/unsubscribable resource (page description) on page 1244
- Memberships – Multi requestable/unsubscribable resource (page description) on page 1246

Multi requestable/unsubscribable resource attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying multi requestable/unsubscribable resource attestation cases on page 537
- Displaying attestors of multi requestable/unsubscribable resource pending attestation cases on page 539

Displaying multi requestable/unsubscribable resource attestation cases

You can see the multi requestable/unsubscribable resource attestation cases

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multi requestable/unsubscribable resources**.
3. On the **Auditing - Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <multi requestable/unsubscribable resource name>** page (see Attestation – Multi requestable/unsubscribable resource (page description) on page 1247).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi requestable/unsubscribable resources (page description) on page 1243
- Auditing - Roles and entitlements: multi requestable/unsubscribable resource (page description) on page 1244

- Attestation – Multi requestable/unsubscribable resource (page description) on page 1247

Displaying attestors of multi requestable/unsubscribable resource pending attestation cases

You can see identities that still have to approve multi requestable/unsubscribable resource attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multi requestable/unsubscribable resources**.
3. On the **Auditing - Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Multi requestable/unsubscribable resources**.
3. On the **Auditing - Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – Multi requestable/unsubscribable resources (page description) on page 1243
- Auditing - Roles and entitlements: multi requestable/unsubscribable resource (page description) on page 1244
- Attestation – Multi requestable/unsubscribable resource (page description) on page 1247

Auditing resources

In One Identity Manager, resources are divided into IT resources and non-IT resources. Non-IT resources are used to establish the working efficiency of identities, such as cell phones, desks, company cars or keys. Resources are assigned to identities directly or by allocation in hierarchical roles. Resources can also be requested.

Resources can own an identity (workstation, device) once only. They can be requested just once. The resources are assigned to identities after approval has been granted and they remain assigned until the request is unsubscribed. You can request them again a later point. Examples are telephone or company car.

You can gather various information about resources.

Detailed information about this topic

- Displaying all resources on page 540
- Displaying resource overviews on page 541
- Displaying resource main data on page 541
- Displaying memberships in resources on page 542
- Resource attestations on page 543
- Displaying role memberships resource members on page 545

Displaying all resources

You can see all the resources.

To display resources

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Resources**.

   This opens the **Auditing - Resources** page (see Auditing - Resources (page description) on page 1248) and displays all the resources.

3. (Optional) To display only resources for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing - Resources (page description) on page 1248

Displaying resource overviews

You can see all relevant information about resources summarized in an overview. The information is represented by shapes in a HyperView.

To display a resource's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Resources**.
3. On the **Auditing - Resources** page, click the resource whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <resource name>** page (see Overview – Resource (page description) on page 1132).

Related topics

- Auditing (page description) on page 1175
- Auditing - Resources (page description) on page 1248
- Auditing - Roles and permissions: resource (page description) on page 1249
- Overview – Resource (page description) on page 1250

Displaying resource main data

You can see resources' main data.

To display a resource's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Resources**.
3. On the **Auditing - Resources** page, click the resource whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <resource name>** page displays the main data (see Main data – Resource (page description) on page 1250).

Related topics

- Auditing (page description) on page 1175
- Auditing - Resources (page description) on page 1248
- Auditing - Roles and permissions: resource (page description) on page 1249
- Main data – Resource (page description) on page 1250

Displaying memberships in resources

You can see identities that have resources assigned to them.

To display identities that are assigned a resource

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Resources**.
3. On the **Auditing - Resources** page, click the resource whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <resource name>** page (see Memberships – Resource (page description) on page 1251).

Related topics

- Auditing (page description) on page 1175
- Auditing - Resources (page description) on page 1248
- Auditing - Roles and permissions: resource (page description) on page 1249
- Memberships – Resource (page description) on page 1251

Resource attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying resource attestation cases on page 543
- Displaying attestors of resource pending attestation cases on page 544

Displaying resource attestation cases

You can see the resources' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Resources**.
3. On the **Auditing - Resources** page, click the resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <resource name>** page (see Attestation - Resource (page description) on page 1252).
6. (Optional) Click on a tab to display the respective attestation cases.

7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing - Resources (page description) on page 1248
- Auditing - Roles and permissions: resource (page description) on page 1249
- Attestation - Resource (page description) on page 1252

Displaying attestors of resource pending attestation cases

You can see identities that still have to approve resource attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Resources**.
3. On the **Auditing - Resources** page, click the resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

6. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Resources**.
3. On the **Auditing - Resources** page, click the resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing - Resources (page description) on page 1248
- Auditing - Roles and permissions: resource (page description) on page 1249
- Attestation - Resource (page description) on page 1252

Displaying role memberships resource members

. You can see which roles and organizations belong to identities that are assigned resources. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a resource

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Resources**.
3. On the **Auditing - Resources** page, click the resource whose members you want to know more about.

4. In the details pane, click **Show details**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <resource name>** page (see Usage – Resource (page description) on page 1253).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Auditing (page description) on page 1175
- Auditing - Resources (page description) on page 1248
- Auditing - Roles and permissions: resource (page description) on page 1249
- Usage – Resource (page description) on page 1253

Auditing software

Software applications can be assigned directly or indirectly to identities. Indirect assignment is carried out by allocating identities and software applications in company structures, like departments, cost centers, locations, or business roles. Examples of software application that can be assigned are: internet, address management, email or text editing software.

You can gather various information about software applications.

Detailed information about this topic

- Displaying all software applications on page 546
- Displaying software application overviews on page 547
- Displaying software application main data on page 548
- Displaying memberships in software applications on page 548
- Software application attestations on page 549
- Displaying role memberships of software application members on page 551

Displaying all software applications

You can see all the software applications.

To display software applications

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Software**.

   This opens the **Auditing - Software** page (see Auditing – Software (page description) on page 1253) and displays all the software applications.
3. (Optional) To display only software for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Software (page description) on page 1253

Displaying software application overviews

You can see all relevant information about software applications summarized in an overview. The information is represented by shapes in a HyperView.

To display a software application's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Software**.
3. On the **Auditing - Software** page, click the software application whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <software application name>** page (see Overview - Software (page description) on page 1255).

Related topics

- Auditing (page description) on page 1175
- Auditing – Software (page description) on page 1253
- Auditing - Roles and permissions: Software (page description) on page 1254
- Overview - Software (page description) on page 1255

Displaying software application main data

You can see software applications' main data.

To display a software application's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Software**.
3. On the **Auditing - Software** page, click the software application whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <software application name>** page displays the main data (see Main data - Software (page description) on page 1255).

Related topics

- Auditing (page description) on page 1175
- Auditing – Software (page description) on page 1253
- Auditing - Roles and permissions: Software (page description) on page 1254
- Main data - Software (page description) on page 1255

Displaying memberships in software applications

You can see identities that have software applications assigned to them.

To display identities that are assigned a software application

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Software**.
3. On the **Auditing - Software** page, click the software application whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <software application name>** page (see Memberships – Software (page description) on page 1256).

Related topics

- Auditing (page description) on page 1175
- Auditing – Software (page description) on page 1253

- Auditing - Roles and permissions: Software (page description) on page 1254
- Memberships – Software (page description) on page 1256

Software application attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying software application attestation cases on page 549
- Displaying attestors of software application pending attestation cases on page 550

Displaying software application attestation cases

You can see the software applications' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Software**.
3. On the **Auditing - Software** page, click the software application whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

This opens the **Attestation - <software application name>** page (see Attestation – Software (page description) on page 1257).

6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – Software (page description) on page 1253
- Auditing - Roles and permissions: Software (page description) on page 1254
- Attestation – Software (page description) on page 1257

Displaying attestors of software application pending attestation cases

You can see identities that still have to approve software attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Software**.
3. On the **Auditing - Software** page, click the software application whose attestation cases you want to display.

4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <software application name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Software**.
3. On the **Auditing - Software** page, click the software application whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <software application name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – Software (page description) on page 1253
- Auditing - Roles and permissions: Software (page description) on page 1254
- Attestation – Software (page description) on page 1257

Displaying role memberships of software application members

. You can see which roles and organizations belong to identities that are assigned software. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a software application

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Software**.
3. On the **Auditing - Software** page, click the software application whose members you want to know more about.
4. In the details pane, click **Show details**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <software application name>** page (see Usage – Software (page description) on page 1258).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Software (page description) on page 1253
- Auditing - Roles and permissions: Software (page description) on page 1254
- Usage – Software (page description) on page 1258

Auditing locations

You can gather various information about locations.

Detailed information about this topic

- Displaying all locations on page 553
- Displaying location overviews on page 553
- Displaying location main data on page 554
- Displaying memberships in locations on page 554
- Displaying location entitlements on page 555
- Location attestations on page 555
- Location compliance on page 558
- Displaying location risk indexes on page 559
- Location history on page 560
- Displaying role memberships of location members on page 563

Displaying all locations

You can see all the locations.

To display locations

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.

   This opens the **Auditing - Locations** page (see Auditing – Locations (page description) on page 1259) and displays all the locations.
3. (Optional) To display only locations for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259

Displaying location overviews

You can see all relevant information about locations summarized in an overview. The information is represented by shapes in a HyperView.

To display a location's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <location name>** page (see Overview - Location (page description) on page 1261).

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259

- Auditing - Roles and permissions: location (page description) on page 1260
- Overview - Location (page description) on page 1261

Displaying location main data

You can see locations' main data.

To display a location's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <location name>** page displays the main data (see Main data - Location (page description) on page 1261).

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- Main data - Location (page description) on page 1261

Displaying memberships in locations

You can see identities that have locations assigned to them.

To display identities that are assigned a location

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <location name>** page (see Memberships – Location (page description) on page 1262).

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- Memberships – Location (page description) on page 1262

Displaying location entitlements

You can see entitlements assigned to locations. You can also display the reason why locations have certain entitlements (entitlement origin).

To display a location's entitlements

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <location name>** page (see Entitlements – Location (page description) on page 1263).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- Entitlements – Location (page description) on page 1263

Location attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to

describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying location attestation cases on page 556
- Displaying attestors of location pending attestation cases on page 557

Displaying location attestation cases

You can see the locations' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <location name>** page (see Auditing– Location (page description) on page 1263).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.

d. (Optional) Click **View current state of the object**

This opens an overview of the attestation.

8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- Auditing– Location (page description) on page 1263

Displaying attestors of location pending attestation cases

You can see identities that still have to approve location attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- Auditing– Location (page description) on page 1263

Location compliance

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying location rule violations on page 559

Displaying location rule violations

You can see location rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose rule violations you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Compliance**.

   This opens the **Compliance - <location name>** page (see Compliance – Location (page description) on page 1265).

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- Compliance – Location (page description) on page 1265

Displaying location risk indexes

You can see location risk indexes.

> NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a cost center's risk index

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose risk index you want to display.
4. In the details pane, click **Show details**.

5. On the overview page, click **Risk**.

   This opens the **Risk - <location name>** page (see Risk – Location (page description) on page 1265).

6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- Risk – Location (page description) on page 1265

Location history

The Web Portal offers you the option to display locations' historical data.

To do this, you have the following options:

Table 41: Historical data

View	Description
Events	This shows you all the events that affect the location, either on a timeline or in a table (see Displaying my locations' history on page 401).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my locations on page 402).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my locations on page 402).

Displaying location history

You can select to display all events involving locations on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose history you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <location name>** page (see History – Location (page description) on page 1266).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.

6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- History – Location (page description) on page 1266

Displaying the status overview of locations

You can see all the changes that affect locations. You can also display how long each change was valid for. Use the status overview to track when changes were made and by

whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose status overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <location name>** page (see History – Location (page description) on page 1266).
6. Click the **Status overview** tab.

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- History – Location (page description) on page 1266

Comparing statuses of locations

You can compare the current state of a location with its state at another time.

To compare states

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose state you want to compare.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.
6. On the **History - <location name>** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Location** page, click the location whose state you want to compare.
4. On the overview page, click **History**.
5. On the **History - <location name>** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- History – Location (page description) on page 1266

Displaying role memberships of location members

. You can see which roles and organizations belong to identities that are assigned locations. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a location

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Locations**.
3. On the **Auditing - Locations** page, click the location whose members you want to know more about.
4. In the details pane, click **Show details**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <location name>** page (see Usage – Location (page description) on page 1268).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.

7. (Optional) To find out which members are assigned to a particular object, click ⓘ (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Auditing (page description) on page 1175
- Auditing – Locations (page description) on page 1259
- Auditing - Roles and permissions: location (page description) on page 1260
- Usage – Location (page description) on page 1268

Auditing system roles

You can gather various information about system roles.

Detailed information about this topic

- Displaying all system roles on page 564
- Displaying system role overviews on page 565
- Displaying system role main data on page 565
- Displaying memberships in system roles on page 566
- Displaying system role entitlements on page 567
- System role attestations on page 567
- System role compliance on page 570
- Displaying system role risk indexes on page 571
- System role history on page 572
- Displaying role memberships of system role members on page 575

Displaying all system roles

You can see all the system roles.

To display system roles

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.

   This opens the **Auditing - System Roles** page (see Auditing – System roles (page description) on page 1269) and displays all the system roles.

3. (Optional) To display only system roles for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269

Displaying system role overviews

You can see all relevant information about system roles summarized in an overview. The information is represented by shapes in a HyperView.

To display a system role's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <system role name>** page (see Overview – System role (page description) on page 1271).

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- Overview – System role (page description) on page 1271

Displaying system role main data

You can see system roles' main data.

To display a system role's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <system role name>** page displays the main data (see Main data – System role (page description) on page 1271).

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- Main data – System role (page description) on page 1271

Displaying memberships in system roles

You can see identities that have system roles assigned to them.

To display identities that are assigned a system role

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <system role name>** page (see Memberships – System role (page description) on page 1272).

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- Memberships – System role (page description) on page 1272

Displaying system role entitlements

You can see entitlements assigned to system roles. You can also display the reason why system roles have certain entitlements (entitlement origin).

To display a system role's entitlements

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <system role name>** page (see Entitlements – System role (page description) on page 1273).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- Entitlements – System role (page description) on page 1273

System role attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying system role attestation cases on page 568
- Displaying attestors of system role pending attestation cases on page 569

Displaying system role attestation cases

You can see the system roles' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <system role name>** page (see Attestation – System role (page description) on page 1273).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.

9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
    a. In the list, click an attestation case.
    b. In the details pane, click the **History** tab.

       This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- Main data – System role (page description) on page 1271

Displaying attestors of system role pending attestation cases

You can see identities that still have to approve system role attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose attestation cases you want to display.
4. In the details pane, click **Show details**.

5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- Main data – System role (page description) on page 1271

System role compliance

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity's Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying system role rule violations on page 571

Displaying system role rule violations

You can see system role rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose rule violations you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Compliance**.

   This opens the **Compliance - <system role name>** page (see Compliance – System role (page description) on page 1275).

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- Compliance – System role (page description) on page 1275

Displaying system role risk indexes

You can see system role risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a system role's risk index

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose risk index you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Risk**.

   This opens the **Risk - <system role name>** page (see Risk – System role (page description) on page 1275).
6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- Risk – System role (page description) on page 1275

System role history

The Web Portal offers you the option to display system roles' historical data.

To do this, you have the following options:

Table 42: Historical data

View	Description
Events	This shows you all the events that affect the system role, either on a timeline or in a table (see Displaying my system roles' history on page 447).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my system roles on page 448).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my system roles on page 448).

Displaying system role history

You can select to display all events involving system roles on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose history you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

This opens the **History - <system role name>** page (see History – System role (page description) on page 1276).

> TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
>
> To zoom in or out, turn the mouse wheel.

6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- History – System role (page description) on page 1276

Displaying the status overview of system roles

You can see all the changes that affect system roles. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.

3. On the **Auditing - System Roles** page, click the system role whose status overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <system role name>** page (see History – System role (page description) on page 1276).
6. Click the **Status overview** tab.

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- History – System role (page description) on page 1276

Comparing statuses of system roles

You can compare the current state of a system role with its state at another time.

To compare states

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose state you want to compare.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.
6. On the **History - <system role name>** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System roles** page, click the system role whose state you want to compare.
4. On the overview page, click **History**.
5. On the **History - <system role name>** page, perform one of the following actions:

- On the timeline, click the event and then **Compare**.
- In the table view, click the event in the list and then in the details pane, click **Compare**.

6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269
- Auditing - Roles and permissions: system role (page description) on page 1270
- History – System role (page description) on page 1276

Displaying role memberships of system role members

You can see which roles and organizations belong to identities that are assigned system roles. . Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a system role

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **System roles**.
3. On the **Auditing - System Roles** page, click the system role whose members you want to know more about.
4. In the details pane, click **Show details**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <system role name>** page (see Usage – System role (page description) on page 1278).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Auditing (page description) on page 1175
- Auditing – System roles (page description) on page 1269

- Auditing - Roles and permissions: system role (page description) on page 1270
- Usage – System role (page description) on page 1278

Auditing system entitlements

NOTE: Auditing of system entitlements is the same for each target system type and is summarized for all target system types in this chapter.

System entitlements map the objects that control access to target system resources in the target systems. A user account obtains the required permissions for accessing target system resources through its memberships in system entitlements.

You can gather various information about system entitlements.

Detailed information about this topic

- Displaying all system entitlements on page 576
- Displaying system entitlement overviews on page 577
- Displaying system entitlement main data on page 577
- Displaying memberships in system entitlements on page 578
- Displaying system entitlement child groups on page 578
- System entitlement attestations on page 579
- System entitlement history on page 581
- Displaying role memberships of system entitlement members on page 584

Displaying all system entitlements

You can see all the system entitlements.

To display system entitlements

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.

   This opens the **Auditing - <target system>** page and displays all associated system entitlements.
3. (Optional) To display only system entitlements for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175

Displaying system entitlement overviews

You can see all relevant information about system entitlements summarized in an overview. The information is represented by shapes in a HyperView.

To display a system entitlement's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <system entitlement name>** page.

Related topics

- Auditing (page description) on page 1175

Displaying system entitlement main data

You can see system entitlements' main data.

To display a system entitlement's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <identity name>** page displays the main data.

Related topics

- Auditing (page description) on page 1175

Displaying memberships in system entitlements

You can see identities that have system entitlements assigned to them.

To display identities that are assigned a system entitlement

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose memberships you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <system entitlement name>** page.

Related topics

- Auditing (page description) on page 1175

Displaying system entitlement child groups

You can display child groups of system entitlements.

To display the child groups of a system entitlement

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose child groups you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Child groups**.

   This opens the **Child groups - <system entitlement name>** page.

Related topics

- Auditing (page description) on page 1175

System entitlement attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying attestation cases of system entitlements on page 579
- Displaying attestors of system entitlement pending attestation cases on page 580

Displaying attestation cases of system entitlements

You can see the system entitlements' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <system entitlement name>** page.
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:

a. In the list, click an attestation case.
b. In the details pane, click **Show details**.
c. In the **Attested object** dialog, select an object in the **Object** menu.

   This shows information about the object.
d. (Optional) Click **View current state of the object**

   This opens an overview of the attestation.

8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175

Displaying attestors of system entitlement pending attestation cases

You can see identities that still have to approve system entitlement attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175

System entitlement history

The Web Portal offers you the option to display system entitlements' historical data.

To do this, you have the following options:

Table 43: Historical data

View	Description
Events	This shows you all the events that affect the system entitlement, either on a timeline or in a table (see Displaying my system entitlements' history on page 426).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status my system entitlements' overview on page 427).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my system entitlements on page 428).

Displaying system entitlement history

You can select to display all events involving system entitlements on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose history you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <system entitlement name>** page.

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.

6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Auditing (page description) on page 1175

Displaying the status overview of system entitlements

You can see all the changes that affect system entitlements. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose status overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.

   This opens the **History - <system entitlement name>** page.
6. Click the **Status overview** tab.

Related topics

- Auditing (page description) on page 1175

Comparing statuses of system entitlements

You can compare the current state of a system entitlement with its state at another time.

To compare states

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose state you want to compare.
4. In the details pane, click **Show details**.
5. On the overview page, click **History**.
6. On the **History - <system entitlement name>** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose state you want to compare.

4. On the overview page, click **History**.
5. On the **History - <system entitlement name>** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Auditing (page description) on page 1175

Displaying role memberships of system entitlement members

You can see which roles and organizations belong to identities that are assigned system entitlements. . Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a system entitlement

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click the appropriate target system.
3. On the **Auditing - <target system>** page, click the system entitlement whose members you want to know more about.
4. In the details pane, click **Show details**.
5. On the overview page, click **Usage**.

    This opens the **Usage - <system entitlement name>** page (see).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Auditing (page description) on page 1175

Auditing assignment resources

Use assignment resources to request hierarchical roles, such as departments or business roles and assign them to identities, devices, and workdesks. For example, you can limit assignment resources to a certain business roles, which makes it unnecessary to select the business role additionally when you request an assignment resource. It is automatically a part of the assignment request.

You can gather various information about assignment resources.

Detailed information about this topic

- Displaying all assignment resources on page 585
- Displaying assignment resource overviews on page 586
- Displaying assignment resource main data on page 586
- Assignment resource attestations on page 587

Displaying all assignment resources

You can see all the assignment resources.

To display assignment resources

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Assignment resources**.

   This opens the **Auditing - Assignment Resources** page (see Auditing - Assignment resource (page description) on page 1279) and displays all the resources.
3. (Optional) To display only assignment resources for which a specific identity is responsible, perform the following actions:
   a. Next to **Select an identity** click **Assign**.
   b. In the **Select an identity** dialog, click the identity.

      TIP: To undo the selection, click Change, and then, in the **Select an identity** dialog, click **Remove assignment**.

Related topics

- Auditing (page description) on page 1175
- Auditing - Assignment resource (page description) on page 1279

Displaying assignment resource overviews

You can see all relevant information about assignment resources summarized in an overview. The information is represented by shapes in a HyperView.

To display an assignment resource's overview

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Assignment resources**.
3. On the **Auditing - Assignment resources** page, click the assignment resource whose overview you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <assignment resource name>** page (see Overview – Assignment resource (page description) on page 1280).

Related topics

- Auditing (page description) on page 1175
- Auditing - Assignment resource (page description) on page 1279
- Auditing - Roles and entitlements: assignment resource (page description) on page 1280
- Overview – Assignment resource (page description) on page 1280

Displaying assignment resource main data

You can see assignment resources' main data.

To display an assignment resource's main data

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Assignment resources**.
3. On the **Auditing - Assignment resources** page, click the assignment resource whose main data you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Main data**.
6. This opens the **Main data - <assignment resource name>** page displays the main data (see Main data – Assignment resource (page description) on page 1281).

Related topics

- Auditing (page description) on page 1175
- Auditing - Assignment resource (page description) on page 1279
- Auditing - Roles and entitlements: assignment resource (page description) on page 1280
- Main data – Assignment resource (page description) on page 1281

Assignment resource attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying assignment resource attestation cases on page 587
- Displaying attestors of assignment resource pending attestation cases on page 588

Displaying assignment resource attestation cases

You can see the assignment resources' attestation cases.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Assignment resources**.

3. On the **Auditing - Assignment resources** page, click the assignment resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <assignment resource name>** page (see Attestation - Assignment resource (page description) on page 1281).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click an attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Auditing (page description) on page 1175
- Auditing - Assignment resource (page description) on page 1279
- Auditing - Roles and entitlements: assignment resource (page description) on page 1280
- Attestation - Assignment resource (page description) on page 1281

Displaying attestors of assignment resource pending attestation cases

You can see identities that still have to approve assignment resource attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Assignment resources**.
3. On the **Auditing - Assignment resources** page, click the assignment resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Auditing**.
2. On the **Auditing** page, click **Assignment resources**.
3. On the **Auditing - Assignment resources** page, click the assignment resource whose attestation cases you want to display.
4. In the details pane, click **Show details**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Auditing (page description) on page 1175
- Auditing - Assignment resource (page description) on page 1279
- Auditing - Roles and entitlements: assignment resource (page description) on page 1280
- Attestation - Assignment resource (page description) on page 1281

Governance administration

In **Governance Administration**, which you reach through **Responsibilities**, you can edit business roles or system entitlements as a target system administrator. You can make the following changes, for example:

- Add a new owner role to an Active Directory group and assign a new product owner.
- Edit an Active Directory group's requestability.
- Modify entitlement properties.

Detailed information about this topic

Managing departments

You can perform a variety of actions on departments and gather information about them.

Detailed information about this topic

- Displaying department risk indexes on page 608
- Department history on page 609
- Displaying role memberships of department members on page 612
- Copying/splitting departments on page 613
- Comparing and merging departments on page 614

Displaying all departments

You can see all the departments.

To display departments

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.

    This opens the **Organization** page (see Organization (page description) on page 1405) and displays all the departments.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405

Restoring deleted departments

You can restore deleted departments. For example, a department can be deleted if two roles are merged during comparison (see Comparing and merging departments on page 614).

To restore a deleted department

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Organization** page, click **Restore a deleted role**.
4. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the department was deleted.
5. Next to the department you want to restore, select the check box.

6. Click **Next**.
7. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
8. Click **Next**.
9. Click **Close**.

To restore a deleted child department

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Organization** page, click the department that was originally parent to the deleted department.
4. In the details pane, click **Edit**.
5. On the overview page, click **Restore**.
6. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the department was deleted.
7. In the list next to the department you want to restore, select the check box.
8. Click **Next**.
9. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
10. Click **Next**.
11. Click **Close**.

Related topics

- Comparing and merging departments on page 614
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406

Displaying department overviews

You can see all relevant information about departments summarized in an overview. The information is represented by shapes in a HyperView.

To display a department's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:

a. Click **Organization**.

b. On the **Organization** page, click **Departments** in the **Type** drop-down.

3. On the **Organization** page, click the department whose overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <department name>** page (see Overview – Department (page description) on page 1408).

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Overview – Department (page description) on page 1408

Displaying and editing department main data

You can see and edit departments' main data.

To show and edit a department's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Organization** page, click the department whose main data you want to display/edit.
4. In the details pane, click **Edit**.
5. On the overview page, click **Main data**.
6. On the **Main data - <department name>**, make your changes in the respective fields (see Main data – Department (page description) on page 1408).
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Main data – Department (page description) on page 1408

Department memberships

Identities can be assigned to departments. You can see these identities, assign further identities to the departments and remove identities from the departments.

Detailed information about this topic

- Displaying department memberships on page 594
- Assigning identities to departments on page 594
- Removing identities from departments on page 595

Displaying department memberships

You can see identities that have departments assigned to them.

To display identities that are assigned a department

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose memberships you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.

    This opens the **Memberships - <department name>** page (see Memberships – Department (page description) on page 1410).

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Memberships – Department (page description) on page 1410

Assigning identities to departments

You can assign departments to identities. You do this through requests.

To assign a department to an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department you want to assign to an identity.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <department name>** page, click **Request memberships**.
7. In the **Request memberships** dialog, in the list, click the identity you want to assign to the department.
8. Click **Add to cart**.
9. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the department.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Memberships – Department (page description) on page 1410

Removing identities from departments

You can remove identities from departments.

To remove an identity from a department

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department you want to remove an identity from.
4. In the details pane, click **Edit**.

5. On the overview page, click **Memberships**.
6. On the **Memberships - <department name>** page, select the check box next to the department that you want to remove.
7. Click **Delete memberships**.

   This cancels the department's assignment.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Memberships – Department (page description) on page 1410

Department entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to system roles you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the departments.

Detailed information about this topic

- Displaying department entitlements on page 596
- Adding department entitlements on page 597
- Deleting department entitlements on page 598

Displaying department entitlements

You can see entitlements assigned to departments. You can also display the reason why departments have certain entitlements (entitlement origin).

To display a department's entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose entitlements you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.

This opens the **Entitlements - <department name>** page (see Entitlements – Department (page description) on page 1411).

6. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Entitlements – Department (page description) on page 1411

Adding department entitlements

You can add entitlements to departments. You do this through a request.

To add an entitlement to a department

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department to which you want to add an entitlement.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.
6. On the **Entitlements - <department name>** page, click **Add new**.
7. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
8. Click **Assign**.
9. In the **Entitlement** dialog, in the list, click the entitlement that you want to add.
10. In the **Add a new entitlement** dialog, click **Request**.
11. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

After the request has been granted approval, the entitlement is added to the department.

Related topics

- Requesting products on page 86
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Entitlements – Department (page description) on page 1411
- My shopping cart (page description) on page 869

Deleting department entitlements

You can delete entitlements assigned to departments.

To delete an entitlement of a department

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose entitlements you want to delete.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.
6. On the **Entitlements - <department name>** page, in the list, select the check box in the row of the entitlement you want to delete.
7. Click **Delete**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Entitlements – Department (page description) on page 1411

Compliance: Departments

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity's Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying department rule violations on page 599
- Displaying department policy violations on page 600
- Displaying rule violations of department members on page 600
- Displaying risk indexes and entitlements of department members on page 601

Displaying department rule violations

You can see department rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance**.

    This opens the **Compliance - <department name>** page (see Compliance – Department (page description) on page 1412).

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Compliance – Department (page description) on page 1412

Displaying department policy violations

You can see department policy violations.

To display policy violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose policy violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <department name>** page (see Compliance reports – Department (page description) on page 1417).
6. In the **View** menu, select **Policy violations**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Compliance reports – Department (page description) on page 1417

Displaying rule violations of department members

You can see the rule violations of identities that are assigned specific departments.

To display rule violations of a department's members

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:

   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <department name>** page (see Compliance reports – Department (page description) on page 1417).
6. In the **View** menu, select **Compliance rule violations**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Compliance reports – Department (page description) on page 1417

Displaying risk indexes and entitlements of department members

For every department, you can see all the identities that have this department as primary or secondary assignment. You can also display the number of entitlements assigned and the risk index.

To display members of a department

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose members you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <department name>** page (see Compliance reports – Department (page description) on page 1417).
6. In the **View** menu, select **Identities: Risk indexes and entitlements**.
7. (Optional) To display more information about an identity, perform the following actions:

a. In the list, click an identity.

b. In the dialog, click **Overview**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Compliance reports – Department (page description) on page 1417

Department attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying department attestation cases on page 602
- Displaying attestors of department pending attestation cases on page 604
- Approving and denying department attestation cases on page 605
- Sending reminders about department pending attestation cases on page 606

Displaying department attestation cases

You can see attestation cases related to departments.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

    This opens the **Attestation - <department name>** page (see Attestation – Department (page description) on page 1412).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click **Show details**.
    c. In the **Attested object** dialog, select an object in the **Object** menu.

        This shows information about the object.
    d. (Optional) Click **View current state of the object**

        This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click the **History** tab.

        This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Attestation – Department (page description) on page 1412

Displaying attestors of department pending attestation cases

You can see identities that still have to approve department attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Attestation – Department (page description) on page 1412

Approving and denying department attestation cases

You can grant or deny approval to attestation cases of departments.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose attestation cases you want to decide approval on.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
7. Click **Approve**.
8. On the **Attestation - <department name>** page, perform one of the following actions:
    - Click (**Approve**) next to the attestation case you want to approve.
    - Click (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
9. Click **Next**.
10. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.

- To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
- For denied attestation cases:
  - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
  - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

11. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Attestation – Department (page description) on page 1412

Sending reminders about department pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:

   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the attestation case that has attestors you want to remind.
8. In the details pane, click **Actions** > **Send a reminder mail**.
9. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
10. Select the email program that you want to use.

    This opens an email template with the attestor's email address.
11. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
7. Click **Send reminder**.
8. In the **Send a reminder mail** dialog, enter the message for the attestor.
9. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.

3. On the **Departments** page, click the department whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <department name>** page, click on a tab to display the corresponding attestation cases
7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
8. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Attestation – Department (page description) on page 1412

Displaying department risk indexes

You can see department risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a department's risk index

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose risk index you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Risk**.

   This opens the **Risk - <department name>** page (see Risk – Department (page description) on page 1085).

6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- Risk assessment on page 209
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Overview – Department (page description) on page 1408

Department history

The Web Portal gives you the option of displaying the historical data of departments for which you are responsible.

To do this, you have the following options:

Table 44: Historical data

View	Description
Events	This shows you all the events that affect the department, either on a timeline or in a table (see Displaying department history on page 609).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of departments on page 611).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of departments on page 611).

Displaying department history

You can select to display all events involving departments on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose history you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

    This opens the **History - <department name>** page (see History – Department (page description) on page 1415).

    TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

    To zoom in or out, turn the mouse wheel.
6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
    - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
    - **Change type**: Only show events on the timeline with the selected change type.
    - **Date**: Only show events on the timeline that took place in the given period.
    - **Properties**: Only show events on the timeline with the selected properties.
    - **Display**: Only show events on the timeline that match the search.
    - **Object**: Only show events on the timeline about the selected object.
7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
    - Click on the event in the timeline.
    - In the table view, click the event and you will see the details in the details pane.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- History – Department (page description) on page 1415

Displaying the status overview of departments

You can see all the changes that affect departments. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose status overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

   This opens the **History - <department name>** page (see History – Department (page description) on page 1415).
6. Click the **Status overview** tab.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- History – Department (page description) on page 1415

Comparing statuses of departments

You can compare the current status of a department that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

6. On the **History** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.
6. On the **History** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
7. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- History – Department (page description) on page 1415

Displaying role memberships of department members

You can see which roles and organizations belong to identities that are assigned departments. . Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a department

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:

a. Click **Organization**.

b. On the **Organization** page, click **Departments** in the **Type** drop-down.

3. On the **Departments** page, click the department whose members you want to know more about.
4. In the details pane, click **Edit**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <department name>** page (see Usage – Department (page description) on page 1417).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click ℹ (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406
- Usage – Department (page description) on page 1417

Copying/splitting departments

You can copy or move memberships and entitlements from departments to new roles (departments, business roles, cost centers, locations).

Any combination of role types is allowed.

To copy a department or move memberships and entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page click the department you want to copy or whose memberships and entitlements you want to move.
4. In the details pane, click **Edit**.
5. On the overview page, click **Split**.
6. In the **Split a role** dialog, in the **Type of the new role** menu, select a type for the new role.

7. Depending on which role type you have selected, enter the corresponding main data of the new role (see Main data – Department (page description) on page 1079, Main data – Business role (page description) on page 1050, Main data – Cost center (page description) on page 1093, or Main data - Location (page description) on page 1106).
8. Click **Next**.
9. Perform the following actions:
   - To neither copy nor move a entitlement/membership to a new role, click **Actions** > **Keep this assignment** next to the corresponding entitlement/membership. Later, the entitlement/membership is only available in the source role.
   - To copy a entitlement/membership to a new role, click **Actions** > **Keep and copy to new role** next to the corresponding entitlement/membership. The entitlement/membership is later included in the source role as well as the target role.
   - To move a entitlement/membership to a new role, click **Actions** > **Move to new role** next to the corresponding entitlement/membership. The entitlement/membership is later removed from the source role and is only included in the target role.
10. Click **Next**.
11. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
12. Click **Next**.
13. Click **Close**.

Related topics

- Department memberships on page 594
- Department entitlements on page 596
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406

Comparing and merging departments

You can compare the properties of departments with the properties of other business roles, departments, cost centers, or locations and then select the properties you require and merge them.

To compare and merge a department

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:

  a. Click **Organization**.
  b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Departments** page, click the department you want to compare and merge.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compare and merge**.
6. In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your department.
7. Click **Assign**.
8. In the **Comparison role** dialog, select the business role/department/cost center/location to compare.

   The assigned memberships and entitlements of both objects are listed with the following information:

   Table 45: Overview of the assignments

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Object</td><td>Shows the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.</td></tr>
<tr><td>Type</td><td>Type of the entitlement/membership.</td></tr>
<tr><td><Name of the source object></td><td rowspan="2">Shows the entitlement/membership's assignment type. The following assignment types are available.
• Direct
• Inherited
• Requested
• Dynamic
• Not assigned
For more detailed information about assigning company resources, see the One Identity Manager Identity Management Base Module Administration Guide.</td></tr>
<tr><td><Name of the compare object></td></tr>
<tr><td>Comparison</td><td>Show you where the entitlement/membership occurs.</td></tr>
</table>

   TIP: To arrange the list of assignments better, use the filters available some of the columns. For more information, see Filtering on page 40..
9. In the **Compare and merge** dialog, click **Merge the selected roles**.
10. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.
12. Click **Close**.

Related topics

- Department memberships on page 594
- Department entitlements on page 596
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406

Displaying department statistics

You can see department statistics. For example, you can see all the identities of a department that have not yet made a request.

To display a department's statistics

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Departments** in the **Type** drop-down.
3. On the **Organization** page, click the department whose statistics you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Statistics**.

    This opens the **Statistics for <department name>** dialog and shows the department's statistics.
6. (Optional) To obtain more information about a chart, click the chart or its header.

Related topics

- Discovering your statistics on the home page on page 795
- Statistics on page 795
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Department (page description) on page 1406

Managing business roles

You can perform a variety of actions on business roles and gather information about them.

Detailed information about this topic

Displaying all business roles

You can see all the business roles.

To display business roles

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.

   This opens the **Business Roles** page (see Business roles (page description) on page 1364) and displays all the business roles.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364

Restoring deleted business roles

You can restore deleted business roles. For example, a business role can be deleted if two roles are merged during comparison (see Comparing and merging business roles on page 639).

To restore a deleted business role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click **Restore a deleted role**.
4. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the business role was deleted.
5. Next to the business role you want to restore, select the check box.
6. Click **Next**.
7. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
8. Click **Next**.
9. Click **Close**.

To restore a deleted child business role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role that was originally parent to the deleted business role.
4. In the details pane, click **Edit**.
5. On the overview page, click **Restore**.
6. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the business role was deleted.
7. In the list next to the business role you want to restore, select the check box.
8. Click **Next**.
9. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
10. Click **Next**.
11. Click **Close**.

Related topics

- Comparing and merging business roles on page 639
- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365

Displaying business role overviews

You can see all relevant information about business roles summarized in an overview. The information is represented by shapes in a HyperView.

To display a business role's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <business role name>** page (see Overview – Business role (page description) on page 1367).

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Overview – Business role (page description) on page 1367

Displaying and editing business role main data

You can see and edit the system roles' main data.

To show and edit a business role's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose main data you want to display/edit.
4. In the details pane, click **Edit**.
5. On the overview page, click **Main data**.
6. On the **Main data - <business role name>**, make your changes in the respective fields (see Main data – Business role (page description) on page 1367).
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Main data – Business role (page description) on page 1367

Business role memberships

Business roles can be assigned identities. You can see these identities, assign further identities to the business roles and remove identities from the business roles.

Detailed information about this topic

- Displaying business role memberships on page 620
- Assigning identities to business roles on page 621
- Removing business roles from identities on page 621

Displaying business role memberships

You can see identities that have business roles assigned to them.

To display identities that are assigned a business role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose memberships you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <business role name>** page (see Memberships – Business role (page description) on page 1368).

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Memberships – Business role (page description) on page 1368

Assigning identities to business roles

You can assign business roles to identities. You do this through requests.

To assign a business role to an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business roles** page, click the business role you want to assign to an identity.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <business role name>** page, click **Request memberships**.
7. In the **Request memberships** dialog, in the list, click the identity you want to assign to the business role.
8. Click **Add to cart**.
9. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the business role.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Memberships – Business role (page description) on page 1368

Removing business roles from identities

You can remove identities from business roles.

To remove an identity from a business role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business roles** page, click the business role you want to remove an identity from.
4. In the details pane, click **Edit**.

5. On the overview page, click **Memberships**.
6. On the **Memberships - <business role name>** page, select the check box next to the business role that you want to remove.
7. Click **Delete memberships**.

   This cancels the business role's assignment.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Memberships – Business role (page description) on page 1368

Business role entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. Assigning identities to business roles avoids you having to assign entitlements separately to each identity. All a business role's entitlements are automatically assigned to all the identities assigned to the business role.

Detailed information about this topic

- Displaying business role entitlements on page 622
- Adding business role entitlements on page 623
- Deleting business role entitlements on page 624

Displaying business role entitlements

You can see entitlements assigned to business roles. You can also display the reason why business roles have certain entitlements (entitlement origin).

To display a business role's entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose entitlements you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <business role name>** page (see Entitlements – Business role (page description) on page 1370).

6. (Optional) To display more information about the origin of an entitlement, perform the following actions:
    a. In the list, click the entitlement that you want to know more about.
    b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

       This displays more information about the entitlement's assignment.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Entitlements – Business role (page description) on page 1370

Adding business role entitlements

You can add entitlements to business roles. You do this through a request.

To add an entitlement to a business role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role to which you want to add an entitlement.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.
6. On the **Entitlements - <business role name>** page, click **Add new**.
7. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
8. Click **Assign**.
9. In the **Entitlement** dialog, in the list, click the entitlement that you want to add.
10. In the **Add a new entitlement** dialog, click **Request**.
11. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    After the request has been granted approval, the entitlement is added to the business role.

Related topics

- Requesting products on page 86
- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Entitlements – Business role (page description) on page 1370
- My shopping cart (page description) on page 869

Deleting business role entitlements

You can delete entitlements assigned to business roles.

To delete an entitlement of a business role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose entitlements you want to delete.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.
6. On the **Entitlements - <business role name>** page, in the list, select the check box in the row of the entitlement you want to delete.
7. Click **Delete**.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Entitlements – Business role (page description) on page 1370

Compliance: Business roles

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity's Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying business role rule violations on page 625
- Displaying business role policy violations on page 626
- Displaying rule violations of business role members on page 626
- Displaying risk indexes and entitlements of business role members on page 627

Displaying business role rule violations

You can see business role rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance**.

   This opens the **Compliance - <business role name>** page (see Compliance – Business role (page description) on page 1371).

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364

- Business role (page description) on page 1365
- Compliance – Business role (page description) on page 1371

Displaying business role policy violations

You can see business role policy violations.

To display policy violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose policy violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <business role name>** page (see Compliance reports – Business role (page description) on page 1376).
6. In the **View** menu, select **Policy violations**.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Compliance reports – Business role (page description) on page 1376

Displaying rule violations of business role members

You can see the rule violations of identities that are assigned specific business roles.

To display rule violations of a business role's members

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <business role name>** page (see Compliance reports – Business role (page description) on page 1376).
6. In the **View** menu, select **Compliance rule violations**.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Compliance reports – Business role (page description) on page 1376

Displaying risk indexes and entitlements of business role members

For every business role, you can see all the identities that have this business role as primary or secondary assignment. You can also display the number of entitlements assigned and the risk index.

To display members of a business role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose members you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <business role name>** page (see Compliance reports – Business role (page description) on page 1376).
6. In the **View** menu, select **Identities: Risk indexes and entitlements**.
7. (Optional) To display more information about an identity, perform the following actions:
   a. In the list, click an identity.
   b. In the dialog, click **Overview**.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Compliance reports – Business role (page description) on page 1376

Business role attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager

attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying business role attestation cases on page 628
- Displaying attestors of business role pending attestation cases on page 629
- Approving and denying business role attestation cases on page 630
- Sending reminders about business role pending attestation cases on page 631

Displaying business role attestation cases

You can see attestation cases related to business roles.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <business role name>** page (see Attestation – Business role (page description) on page 1371).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:

a. In the list, click the attestation case.
b. In the details pane, click **Show details**.
c. In the **Attested object** dialog, select an object in the **Object** menu.

   This shows information about the object.
d. (Optional) Click **View current state of the object**

   This opens an overview of the attestation.

8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Attestation – Business role (page description) on page 1371

Displaying attestors of business role pending attestation cases

You can see identities that still have to approve business role attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the (pending) attestation case that has attestors you want to display.

8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Attestation – Business role (page description) on page 1371

Approving and denying business role attestation cases

You can grant or deny approval to attestation cases of business roles.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to decide approval on.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
7. Click **Approve**.

8. On the **Pending Attestations - <business role name>** page, perform one of the following actions:
    - Click (**Approve**) next to the attestation case you want to approve.
    - Click (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
9. Click **Next**.
10. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
11. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Attestation – Business role (page description) on page 1371

Sending reminders about business role pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the attestation case that has attestors you want to remind.
8. In the details pane, click **Actions** > **Send a reminder mail**.
9. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
10. Select the email program that you want to use.

    This opens an email template with the attestor's email address.
11. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
7. Click **Send reminder**.
8. In the **Send a reminder mail** dialog, enter the message for the attestor.
9. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <business role name>** page, click on a tab to display the corresponding attestation cases
7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
8. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Attestation – Business role (page description) on page 1371

Displaying business role risk indexes

You can see business role risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a business role's risk index

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose risk index you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Risk**.

This opens the **Risk - <business role name>** page (see Risk – Business role (page description) on page 1056).

6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- Risk assessment on page 209
- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Overview – Business role (page description) on page 1367

Business role history

The Web Portal gives you the option of displaying the historical data of business roles for which you are responsible.

To do this, you have the following options:

Table 46: Historical data

View	Description
Events	This shows you all the events that affect the business role, either on a timeline or in a table (see Displaying business role history on page 634).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of business roles on page 635).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of business roles on page 636).

Displaying business role history

You can select to display all events involving business roles on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose history you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

   This opens the **History - <business role name>** page (see History – Business role (page description) on page 1374).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.
6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- History – Business role (page description) on page 1374

Displaying the status overview of business roles

You can see all the changes that affect business roles. You can also display how long each change was valid for. Use the status overview to track when changes were made and by

whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose status overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

   This opens the **History - <business role name>** page (see History – Business role (page description) on page 1374).
6. Click the **Status overview** tab.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- History – Business role (page description) on page 1374

Comparing statuses of business roles

You can compare the current status of a business role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.
6. On the **History** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.
6. On the **History** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
7. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- History – Business role (page description) on page 1374

Displaying role memberships of business role members

You can see which roles and organizations belong to identities that are assigned business roles. . Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a business role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role whose members you want to know more about.
4. In the details pane, click **Edit**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <business role name>** page (see Usage – Business role (page description) on page 1376).

6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365
- Usage – Business role (page description) on page 1376

Copying/splitting business roles

You can copy or move memberships and entitlements from business roles to new roles (departments, business roles, cost centers, locations).

Any combination of role types is allowed.

To copy a business role or move memberships and entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business Roles** page, click the business role you want to copy or whose memberships and entitlements you want to move.
4. In the details pane, click **Edit**.
5. On the overview page, click **Split**.
6. In the **Split a role** dialog, in the **Type of the new role** menu, select a type for the new role.
7. Depending on which role type you have selected, enter the corresponding main data of the new role (see Main data – Department (page description) on page 1079, Main data – Business role (page description) on page 1050, Main data – Cost center (page description) on page 1093, or Main data - Location (page description) on page 1106).
8. Click **Next**.
9. Perform the following actions:
    - To neither copy nor move a entitlement/membership to a new role, click **Actions** > **Keep this assignment** next to the corresponding entitlement/membership. Later, the entitlement/membership is only available in the source role.

- To copy a entitlement/membership to a new role, click **Actions** > **Keep and copy to new role** next to the corresponding entitlement/membership. The entitlement/membership is later included in the source role as well as the target role.
- To move a entitlement/membership to a new role, click **Actions** > **Move to new role** next to the corresponding entitlement/membership. The entitlement/membership is later removed from the source role and is only included in the target role.

10. Click **Next**.
11. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
12. Click **Next**.
13. Click **Close**.

Related topics

- Business role memberships on page 620
- Business role entitlements on page 622
- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365

Comparing and merging business roles

You can compare the properties of business roles with the properties of other business roles, departments, cost centers, or locations and then select the properties you require and merge them.

To compare and merge a business role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Business Roles**.
3. On the **Business roles** page, click the business role that you want to compare and merge.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compare and merge**.
6. In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your business role.
7. Click **Assign**.

8. In the **Comparison role** dialog, select the business role/department/cost center/location to compare.

   The assigned memberships and entitlements of both objects are listed with the following information:

   Table 47: Overview of the assignments

<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Object</td><td>Shows the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.</td></tr>
<tr><td>Type</td><td>Type of the entitlement/membership.</td></tr>
<tr><td><Name of the source object></td><td rowspan="2">Shows the entitlement/membership's assignment type. The following assignment types are available.
• Direct
• Inherited
• Requested
• Dynamic
• Not assigned
For more detailed information about assigning company resources, see the One Identity Manager Identity Management Base Module Administration Guide.</td></tr>
<tr><td><Name of the compare object></td></tr>
<tr><td>Comparison</td><td>Show you where the entitlement/membership occurs.</td></tr>
</table>

   TIP: To arrange the list of assignments better, use the filters available some of the columns. For more information, see Filtering on page 40..

9. In the **Compare and merge** dialog, click **Merge the selected roles**.
10. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.
12. Click **Close**.

Related topics

- Business role memberships on page 620
- Business role entitlements on page 622
- Governance administration (page description) on page 1363
- Business roles (page description) on page 1364
- Business role (page description) on page 1365

Managing identities

You can perform a variety of actions on identities and gather information about them.

Detailed information about this topic

- Displaying all identities on page 641
- Adding identities on page 642
- Displaying identity overviews on page 643
- Displaying and editing identity main data on page 643
- Assigning other managers to identities on page 644
- Creating reports about identities on page 645
- Displaying identity requests on page 645
- Identity entitlements on page 646
- Identity delegations on page 647
- Identity attestations on page 650
- Displaying identity risk indexes on page 655
- Identity history on page 656
- Creating passcodes for identities on page 659

Displaying all identities

You can see all the identities.

To display identities

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.

   This opens the **Identities** page (see Identities (page description) on page 1378) and displays all the identities.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378

Adding identities

You can add new identities. This function is mainly designed for adding external identities. For example, subcontractors who are not entered in the human resources department. Data from new identities is either transferred completely to the database or existing data is updated and/or augmented. This depends on the system configuration and the import setting from closed systems.

To add a new identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click **Add a new identity**.
4. On the **Add a new identity** page, enter the identity's main data in the respective fields (see Adding a new identity (page description) on page 1379).
5. Click **Save**.

   When saving, the system checks whether the combination of first and last name already exists.
6. Depending on the result of checking the name combination, perform one of the following actions:
   - If this combination of names does not yet exist, confirm the prompt with **Yes**.
   - If this combination of names already exists and you want to edit/update the existing identity:
     1. On the **Other identities with similar properties** page, in the list, click the identity that you want to edit/update.
     2. Click **Update identity data**.
     3. Confirm the prompt with **Yes** in the dialog.

        This edits/updates the identity data.
   - If identical combinations already exists and you still want add a new identity:
     1. On the **Other identities with similar properties** page, click **Add a new identity**.
     2. Confirm the prompt with **Yes** in the dialog.

        This adds new identity data.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Adding a new identity (page description) on page 1379

Displaying identity overviews

You can see all relevant information about identities summarized in an overview. For example, this information includes identities, requests, rule violations, user accounts, subidentities, assigned permissions, and memberships. The information is represented by shapes in a HyperView.

To display an identity's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <identity's name>** page (see Overview – Identity (page description) on page 1382).

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Overview – Identity (page description) on page 1382

Displaying and editing identity main data

You can see and edit identities' main data.

To show and edit an identity's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <identity's name>**, make your changes in the respective fields (see Main data – Identity (page description) on page 1382).
6. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378

- Identity (page description) on page 1380
- Main data – Identity (page description) on page 1382

Assigning other managers to identities

You can assign identities to other managers.

To assign an identity to a new manager

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity that you want to assign to a new manager.
4. On the overview page, click **Main data**.
5. On the **Main data - <identity's name>**, click **Assign to new manager**.
6. On the **Assign New Manager** page, next to **New manager**, click **Assign**/**Change**.
7. In the **New manager** dialog box, click the manager you want to assign to the identity.
8. On the **Assign to new manager** page, in the **Effective date** field, set a date and time from which the new manager takes effect.
9. If the identity for whom you have selected the new manager, already has approved requests or entitlements, these are deleted automatically on this date. If you want the identity to retain these requests or entitlements when transferring to the new manager, deselect the check boxes next to the respective requests or entitlements.
10. Click **Submit**.
11. In the dialog, confirm the prompt with **Yes**.

    NOTE: Your request to change managers is presented to the approver responsible for approval on the **Pending Requests** page (see Approving new managers' pending requests on page 117).

Related topics

- Approving new managers' pending requests on page 117
- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Main data – Identity (page description) on page 1382
- Assigning to new manager (page description) on page 1384

Creating reports about identities

You can create reports using the data from identities.

To create a report about an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity for which you want to create a report.
4. On the overview page, click **Main data**.
5. On the **Main data - <identity's name>**, click **Generate report**.
6. In the dialog, select one or both of the check boxes.
   - **Generate report including history**: A history with all changes to the identity is attached to the report.
   - **Include data for sub identities in the report**: The report additionally includes data for all the identity's sub identities.
7. Click **Generate report**.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Main data – Identity (page description) on page 1382

Displaying identity requests

You can display requests made by identities. All requests that identities have made themselves or that have been made for them (for example, by a manager) are displayed.

To display requests of an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose requests you want to display.
4. On the overview page, click **Requests**.

   This opens the**Requests- <name of identity>** page (see Requests - Identities ((page description)) on page 1385).
5. (Optional) Click **Advanced Search** to control which requests are displayed (see Requests - Identities ((page description)) on page 1385). For example, you can display only pending (not yet assigned) requests.

Related topics

- Displaying request history on page 128
- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Requests - Identities ((page description)) on page 1385

Identity entitlements

Identities can have a variety of entitlements. You can see these entitlements and delete them.

Detailed information about this topic

- Displaying identity entitlements on page 646
- Deleting identity entitlements on page 647

Displaying identity entitlements

You can see entitlements assigned to identities. You can also display the reason why identities have certain entitlements (entitlement origin).

To display an identity's entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose entitlements you want to display.
4. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <identity's name>** page (see Entitlements – Identity (page description) on page 1387).
5. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Entitlements – Identity (page description) on page 1387

Deleting identity entitlements

You can delete entitlements assigned to identities.

To delete an entitlement of an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose delegation you want to delete.
4. On the overview page, click **Entitlements**.
5. On the **Entitlements - <identity>** page, in the list, select the check box in the row of the entitlement you want to delete.
6. Click **Delete memberships**.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Entitlements – Identity (page description) on page 1387

Identity delegations

Responsibilities or roles of identities can be temporarily delegated to other identities. For example, the responsibility for a department can be given to another identity.

Detailed information about this topic

- Displaying identity delegations on page 648
- Adding delegations for identities on page 648
- Canceling identity delegations on page 649
- Deleting identities' delegations on page 649

Displaying identity delegations

You can see the identities' delegations.

To display delegations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose delegations you want to display.
4. On the overview page, click **Delegations**.

   This opens the **Delegations - <identity's name>** page (see Delegations – Identity (page description) on page 1388).

- Displaying delegations on page 458
- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Delegations – Identity (page description) on page 1388

Adding delegations for identities

You can delegate role memberships and responsibilities to other identities. For example, you can give one identity's responsibility for a department to another identity.

> NOTE: You cannot edit a delegation afterward. If you want to make a change to the delegation, delete the it (see Deleting identities' delegations on page 649) and create a new delegation.

To create a delegation

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity who should become the delegate.
4. On the overview page, click **Delegations**.
5. On the **Delegations - <identity's name>**, click **New delegation**.
6. Click **Next**.
7. In the step, in the list, select the check boxes in front of the role memberships/responsibilities you want to delegate.
8. Click **Next**.
9. In the **Add additional information** set, configure the following settings:
   - **Valid from**: Specify from when the role/responsibility will be delegated.
   - **Valid until**: Specify until when the role/responsibility will be delegated.

- **Notify me if the recipient of the delegation makes a decision**: (Optional) Select the check box if you want to be notified when the recipient makes an approval decision about a delegated role/responsibility.
- **The recipient can delegate this role**: (Optional) Select the check box to specify that the recipient can delegate their delegated role/responsibility on to another identity.
- **Reason**: (Optional) In the dialog, enter a reason for the delegation.
- **Priority**: (Optional) In the menu, select a priority for the delegation.

10. Click **Save**.

- Creating delegations on page 459
- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Delegations – Identity (page description) on page 1388

Canceling identity delegations

You can cancel existing delegations of identities.

NOTE: You can only cancel delegations as long they have the **Request** or **Approved** status. You can delete delegations with the **Assigned** status (see Deleting identities' delegations on page 649).

To cancel a delegation

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose delegation you want to cancel.
4. On the overview page, click **Delegations**.

- Canceling delegations on page 460
- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Delegations – Identity (page description) on page 1388

Deleting identities' delegations

You can delete the identities' delegations.

NOTE: You can only delete delegations as long as they have the **Assigned** status. You can cancel delegations that have the **Request** or **Approved** status (see Canceling identity delegations on page 649).

To delete a delegation

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose delegation you want to delete.
4. On the overview page, click **Delegations**.

- Deleting delegations on page 461
- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Delegations – Identity (page description) on page 1388

Identity attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying identity attestation cases on page 650
- Displaying attestors of identity pending attestation cases on page 651
- Approving and denying identity attestation cases on page 652
- Sending reminders about identity pending attestation cases on page 654

Displaying identity attestation cases

You can see attestation cases related to identities.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <identity's name>** page (see Attestation – Identity (page description) on page 1389).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Attestation – Identity (page description) on page 1389

Displaying attestors of identity pending attestation cases

You can see identities that still have to approve identities attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity's name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity's name>** page, click on a tab to display the corresponding attestation cases.
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Attestation – Identity (page description) on page 1389

Approving and denying identity attestation cases

You can grant or deny approval to attestation cases of identities.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want decide approval on.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity's name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Approve**.
7. On the **Pending Attestations - <identity's name>** page, perform one of the following actions:
    - Click (**Approve**) next to the attestation case you want to approve.
    - Click (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363

- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Attestation – Identity (page description) on page 1389

Sending reminders about identity pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity's name>** page, click on a tab to display the corresponding attestation cases.
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.

3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity's name>** page, click on a tab to display the corresponding attestation cases.
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <identity's name>** page, click on a tab to display the corresponding attestation cases.
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Attestation – Identity (page description) on page 1389

Displaying identity risk indexes

You can see identities risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display an identity's risk index

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose risk index you want to display.
4. On the overview page, click **Risk**.

   This opens the **Risk - <identity's name>** page (see Risk – Identity (page description) on page 1029).
5. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- Risk assessment on page 209
- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- Overview – Identity (page description) on page 1382

Identity history

The Web Portal gives you the option of displaying the historical data of identities for which you are responsible.

To do this, you have the following options:

Table 48: Historical data

View	Description
Events	This shows you all the events that affect the identity, either on a timeline or in a table (see Displaying identity history on page 657).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of identities on page 658).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of identities on page 658).

Displaying identity history

You can select to display all events involving identities on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose history you want to display.
4. On the overview page, click **History**.

   This opens the **History - <identity's name>** page (see History – Identity (page description) on page 1392).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.
5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- History – Identity (page description) on page 1392

Displaying the status overview of identities

You can see all the changes that affect identities. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <identity's name>** page (see History – Identity (page description) on page 1392).
5. Click the **Status overview** tab.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- History – Identity (page description) on page 1392

Comparing statuses of identities

You can compare the current status of an identity that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380
- History – Identity (page description) on page 1392

Creating passcodes for identities

If identities have forgotten their password for logging into the Web Portal and the passwords cannot be reset with the question and answer feature, you can create passcodes for them. With this passcode, identities can log on to the Password Reset Portal once and for a limited time.

To create a passcode for an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Identities**.
3. On the **Identities** page, click the identity for which you want to create the passcode.
4. On the overview page, click **Passcode**.

    The generated passcode, its validity period, and a URL that the identity uses to login in to thePassword Reset Portal, are displayed in a dialog.
5. Note or copy the code and have it sent to the identity with the validity period.

Related topics

- Governance administration (page description) on page 1363
- Identities (page description) on page 1378
- Identity (page description) on page 1380

Managing cost centers

You can perform a variety of actions on cost centers and gather information about them.

Detailed information about this topic

- Displaying all cost centers on page 660
- Restoring deleted cost centers on page 661
- Displaying cost center overviews on page 662
- Displaying and editing cost center main data on page 662
- Cost center memberships on page 663
- Cost center entitlements on page 665
- Compliance: Cost centers on page 668
- Cost center attestations on page 671
- Displaying cost center risk indexes on page 677
- Cost center history on page 678
- Displaying role memberships of cost center members on page 682
- Copying/splitting cost centers on page 682
- Comparing and merging cost centers on page 684

Displaying all cost centers

You can see all the cost centers.

To display cost centers

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.

   This opens the **Organization** page (see Organization (page description) on page 1405) and displays all the cost centers.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405

Restoring deleted cost centers

You can restore deleted cost centers. For example, a cost center can be deleted if two roles are merged during comparison (see Comparing and merging cost centers on page 684).

To restore a deleted cost center

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Organization** page, click **Restore a deleted role**.
4. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the cost center was deleted.
5. Next to the cost center you want to restore, select the check box.
6. Click **Next**.
7. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
8. Click **Next**.
9. Click **Close**.

To restore a deleted child cost center

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Organization** page, click the cost center that was originally parent to the deleted cost center.
4. In the details pane, click **Edit**.
5. On the overview page, click **Restore**.
6. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the cost center was deleted.
7. In the list next to the cost center you want to restore, select the check box.
8. Click **Next**.
9. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
10. Click **Next**.
11. Click **Close**.

Related topics

- Comparing and merging cost centers on page 684
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419

Displaying cost center overviews

You can see all relevant information about cost centers summarized in an overview. The information is represented by shapes in a HyperView.

To display a cost center's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Organization** page, click the cost center whose overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Overview**.

    This opens the **Overview - <cost center name>** page (see Overview – Cost center (page description) on page 1421).

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Overview – Cost center (page description) on page 1421

Displaying and editing cost center main data

You can see and edit cost centers' main data.

To show and edit a cost center's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:

    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Organization** page, click the cost center whose main data you want to display/edit.
4. In the details pane, click **Edit**.
5. On the overview page, click **Main data**.
6. On the **Main data - <cost center>**, make your changes in the respective fields (see Main data – Cost center (page description) on page 1421).
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Main data – Cost center (page description) on page 1421

Cost center memberships

Identities can be assigned to cost centers. You can see these identities, assign further identities to the cost centers and remove identities from the cost centers.

Detailed information about this topic

- Displaying cost center memberships on page 663
- Assigning identities to cost centers on page 664
- Removing identities from cost centers on page 665

Displaying cost center memberships

You can see identities that have cost centers assigned to them.

To display identities that are assigned a cost center

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose memberships you want to display.

4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <cost center name>** page (see Memberships – Cost center (page description) on page 1422).

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Memberships – Cost center (page description) on page 1422

Assigning identities to cost centers

You can assign cost centers to identities. You do this through requests.

To assign a cost center to an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center you want to assign to an identity.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <cost center name>** page, click **Request memberships**.
7. In the **Request memberships** dialog, in the list, click the identity you want to assign to the cost center.
8. Click **Add to cart**.
9. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the cost center.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405

- Cost center (page description) on page 1419
- Memberships – Cost center (page description) on page 1422

Removing identities from cost centers

You can remove identities from cost centers.

To remove an identity from a cost center

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center you want to remove an identity from.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <cost center name>** page, select the check box next to the cost center that you want to remove.
7. Click **Delete memberships**.

   This cancels the cost center's assignment.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Memberships – Cost center (page description) on page 1422

Cost center entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to cost centers you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the cost centers.

Detailed information about this topic

- Displaying cost center entitlements on page 666
- Adding cost center entitlements on page 666
- Deleting cost center entitlements on page 667

Displaying cost center entitlements

You can see entitlements assigned to cost centers. You can also display the reason why cost centers have certain entitlements (entitlement origin).

To display a cost center's entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose entitlements you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <cost center name>** page (see Entitlements – Cost center (page description) on page 1423).
6. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Entitlements – Cost center (page description) on page 1423

Adding cost center entitlements

You can add entitlements to cost centers. You do this through a request.

To add an entitlement to a cost center

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.

3. On the **Cost Centers** page, click the cost center to which you want to add an entitlement.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.
6. On the **Entitlements - <cost center name>** page, click **Add new**.
7. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
8. Click **Assign**.
9. In the **Entitlement** dialog, in the list, click the entitlement that you want to add.
10. In the **Add a new entitlement** dialog, click **Request**.
11. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    After the request has been granted approval, the entitlement is added to the cost center.

Related topics

- Requesting products on page 86
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Entitlements – Cost center (page description) on page 1423
- My shopping cart (page description) on page 869

Deleting cost center entitlements

You can delete entitlements assigned to cost centers.

To delete an entitlement of a cost center

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose entitlements you want to delete.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.

6. On the **Entitlements - <cost center name>** page, in the list, select the check box in the row of the entitlement you want to delete.
7. Click **Delete**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Entitlements – Cost center (page description) on page 1423

Compliance: Cost centers

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity’s Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying cost center rule violations on page 669
- Displaying cost center policy violations on page 669
- Displaying rule violations of cost center members on page 670
- Displaying risk indexes and entitlements of cost center members on page 670

Displaying cost center rule violations

You can see cost center rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance**.

   This opens the **Compliance - <cost center name>** page (see Compliance – Cost center (page description) on page 1424).

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Compliance – Cost center (page description) on page 1424

Displaying cost center policy violations

You can see cost center policy violations.

To display policy violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose policy violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <cost center name>** page (see Compliance reports – Cost center (page description) on page 1430).
6. In the **View** menu, select **Policy violations**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Compliance reports – Cost center (page description) on page 1430

Displaying rule violations of cost center members

You can see the rule violations of identities that are assigned specific cost centers.

To display rule violations of a cost center's members

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

    This opens the **Compliance reports - <cost center name>** page (see Compliance reports – Cost center (page description) on page 1430).
6. In the **View** menu, select **Compliance rule violations**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Compliance reports – Cost center (page description) on page 1430

Displaying risk indexes and entitlements of cost center members

For every cost center, you can see all the identities that have this cost center as primary or secondary assignment. You can also display the number of entitlements assigned and the risk index.

To display members of a cost center

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose members you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <cost center name>** page (see Compliance reports – Cost center (page description) on page 1430).
6. In the **View** menu, select **Identities: Risk indexes and entitlements**.
7. (Optional) To display more information about an identity, perform the following actions:
   a. In the list, click an identity.
   b. In the dialog, click **Overview**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Compliance reports – Cost center (page description) on page 1430

Cost center attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying cost center attestation cases on page 672
- Displaying attestors of cost center pending attestation cases on page 673
- Approving and denying cost center attestation cases on page 674
- Sending reminders about cost center pending attestation cases on page 676

Displaying cost center attestation cases

You can see attestation cases related to cost centers.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <cost center name>** page (see Attestation – Cost center (page description) on page 1425).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:

   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Attestation – Cost center (page description) on page 1425

Displaying attestors of cost center pending attestation cases

You can see identities that still have to approve cost center attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <cost center role name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

    The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Attestation – Cost center (page description) on page 1425

Approving and denying cost center attestation cases

You can grant or deny approval to attestation cases of cost centers.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose attestation cases you want to decide approval on.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.

7. Click **Approve**.
8. On the **Attestation - <cost center name>** page, perform one of the following actions:
    - Click ☑ (**Approve**) next to the attestation case you want to approve.
    - Click ☒ (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
9. Click **Next**.
10. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
11. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Attestation – Cost center (page description) on page 1425

Sending reminders about cost center pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the attestation case that has attestors you want to remind.
8. In the details pane, click **Actions** > **Send a reminder mail**.
9. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
10. Select the email program that you want to use.

    This opens an email template with the attestor's email address.
11. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.

3. On the **Cost Centers** page, click the cost center whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Send reminder**.
8. In the **Send a reminder mail** dialog, enter the message for the attestor.
9. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <cost center name>** page, click on a tab to display the corresponding attestation cases.
7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
8. Select the email program that you want to use.

    This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Attestation – Cost center (page description) on page 1425

Displaying cost center risk indexes

You can see cost center risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a cost center's risk index

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose risk index you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Risk**.

    This opens the **Risk - <cost center name>** page (see Risk – Cost center (page description) on page 1099).
6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- Risk assessment on page 209
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Overview – Cost center (page description) on page 1421

Cost center history

The Web Portal gives you the option of displaying the historical data of cost centers for which you are responsible.

To do this, you have the following options:

Table 49: Historical data

View	Description
Events	This shows you all the events that affect the cost center, either on a timeline or in a table (see Displaying cost center history on page 679).
Status overview	This shows you an overview of all assignments. It also shows how

View	Description
	long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of cost centers on page 680).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of cost centers on page 681).

Displaying cost center history

You can select to display all events involving cost centers on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose history you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

    This opens the **History - <cost center name>** page (see History – Cost center (page description) on page 1428).

    TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

    To zoom in or out, turn the mouse wheel.
6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
    - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
    - **Change type**: Only show events on the timeline with the selected change type.
    - **Date**: Only show events on the timeline that took place in the given period.
    - **Properties**: Only show events on the timeline with the selected properties.
    - **Display**: Only show events on the timeline that match the search.
    - **Object**: Only show events on the timeline about the selected object.

7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- History – Cost center (page description) on page 1428

Displaying the status overview of cost centers

You can see all the changes that affect cost centers. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose status overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

   This opens the **History - <cost center name>** page (see History – Cost center (page description) on page 1428).
6. Click the **Status overview** tab.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- History – Cost center (page description) on page 1428

Comparing statuses of cost centers

You can compare the current status of a cost center that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.
6. On the **History** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.
6. On the **History** page, perform one of the following actions:
    - On the timeline, click the event and then **Compare**.
    - In the table view, click the event in the list and then in the details pane, click **Compare**.
7. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405

- Cost center (page description) on page 1419
- History – Cost center (page description) on page 1428

Displaying role memberships of cost center members

You can see which roles and organizations belong to identities that are assigned cost centers. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a cost center

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center whose members you want to know more about.
4. In the details pane, click **Edit**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <cost center name>** page (see Usage – Cost center (page description) on page 1430).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419
- Usage – Cost center (page description) on page 1430

Copying/splitting cost centers

You can copy or move memberships and entitlements from cost centers to new roles (departments, business roles, cost centers, locations).

Any combination of role types is allowed.

To copy a cost center or move memberships and entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center you want to copy or whose memberships and entitlements you want to move.
4. In the details pane, click **Edit**.
5. On the overview page, click **Split**.
6. In the **Split a role** dialog, in the **Type of the new role** menu, select a type for the new role.
7. Depending on which role type you have selected, enter the corresponding main data of the new role (see Main data – Department (page description) on page 1079, Main data – Business role (page description) on page 1050, Main data – Cost center (page description) on page 1093, or Main data - Location (page description) on page 1106).
8. Click **Next**.
9. Perform the following actions:
   - To neither copy nor move a entitlement/membership to a new role, click **Actions** > **Keep this assignment** next to the corresponding entitlement/membership. Later, the entitlement/membership is only available in the source role.
   - To copy a entitlement/membership to a new role, click **Actions** > **Keep and copy to new role** next to the corresponding entitlement/membership. The entitlement/membership is later included in the source role as well as the target role.
   - To move a entitlement/membership to a new role, click **Actions** > **Move to new role** next to the corresponding entitlement/membership. The entitlement/membership is later removed from the source role and is only included in the target role.
10. Click **Next**.
11. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
12. Click **Next**.
13. Click **Close**.

Related topics

- Cost center memberships on page 663
- Cost center entitlements on page 665

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419

Comparing and merging cost centers

You can compare the properties of cost centers with the properties of other business roles, departments, cost centers, or locations and then select the properties you require and merge them.

To compare and merge a cost center

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Cost Centers** page, click the cost center you want to compare and merge.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compare and merge**.
6. In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your cost center.
7. Click **Assign**.
8. In the **Comparison role** dialog, select the business role/department/cost center/location to compare.

    The assigned memberships and entitlements of both objects are listed with the following information:

Table 50: Overview of the assignments

Column	Description
Object	Shows the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.
Type	Type of the entitlement/membership.
<Name of the source object>	Shows the entitlement/membership's assignment type. The following assignment types are available. • Direct • Inherited • Requested

Column	Description
	• Dynamic • Not assigned
<Name of the compare object>	For more detailed information about assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.
Comparison	Show you where the entitlement/membership occurs.

TIP: To arrange the list of assignments better, use the filters available some of the columns. For more information, see Filtering on page 40..

9. In the **Compare and merge** dialog, click **Merge the selected roles**.
10. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.
12. Click **Close**.

Related topics

- Cost center memberships on page 663
- Cost center entitlements on page 665
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Cost center (page description) on page 1419

Displaying cost center statistics

You can see cost center statistics.

To display a cost center's statistics

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Cost centers** in the **Type** drop-down.
3. On the **Organization** page, click the cost center whose statistics you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Statistics**.

   This opens the **Statistics for <cost center name>** dialog and shows the cost center's statistics.

6. (Optional) To obtain more information about a chart, click the chart or its header.

Related topics

- Discovering your statistics on the home page on page 795
- Statistics on page 795
- Organization (page description) on page 1405
- Cost center (page description) on page 1419

Managing multi-request resources

You can perform a variety of actions on multi-request resources and gather information about them.

Detailed information about this topic

- Displaying multi-request resources on page 686
- Displaying multi-request resource overviews on page 687
- Displaying and editing multi-request resources main data on page 687
- Multi-request resource attestations on page 688

Displaying multi-request resources

You can see all the multi-request resources.

To display multi-request resources

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.

   This opens the **Multi-request Resources** page (see Multi-request resources (page description) on page 1394) and displays all the multi-request resources.

Related topics

- Governance administration (page description) on page 1363
- Multi-request resources (page description) on page 1394

Displaying multi-request resource overviews

You can see all relevant information about multi-request resources summarized in an overview. The information is represented by shapes in a HyperView.

To display a multi-request resource's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <multi-request resource name>** page (see Overview – Multi-request resource (page description) on page 1395).

Related topics

- Governance administration (page description) on page 1363
- Multi-request resources (page description) on page 1394
- Multi-request resource (page description) on page 1395
- Overview – Multi-request resource (page description) on page 1395

Displaying and editing multi-request resources main data

You can see and edit multi-request resources' main data.

To show and edit a multi-request resource's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose main data you want to show/edit.
4. In the details pane, click **Edit**.
5. On the overview page, click **Main data**.
6. On the **Main data - <multi-request resource name>**, make your changes in the respective fields (see Main data – Multi-request resource (page description) on page 1396).
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- Multi-request resources (page description) on page 1394
- Multi-request resource (page description) on page 1395
- Main data – Multi-request resource (page description) on page 1396

Multi-request resource attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying multi-request resource attestation cases on page 688
- Displaying attestors of multi-request resource pending attestation cases on page 690
- Approving and denying multi-request resource attestation cases on page 691
- Sending reminders about multi-request resource pending attestation cases on page 692

Displaying multi-request resource attestation cases

You can see attestation cases related to multi-request resources.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <multi-request resource name>** page (see Attestation – Multi-request resource (page description) on page 1397).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- Multi-request resources (page description) on page 1394
- Multi-request resource (page description) on page 1395
- Attestation – Multi-request resource (page description) on page 1397

Displaying attestors of multi-request resource pending attestation cases

You can see identities that still have to approve multi-request resource attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- Multi-request resources (page description) on page 1394
- Multi-request resource (page description) on page 1395
- Attestation – Multi-request resource (page description) on page 1397

Approving and denying multi-request resource attestation cases

You can grant or deny approval to attestation cases of multi-request resources.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to decide approval on.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Approve**.
8. On the **Attestation - <multi-request resource name>** page, perform one of the following actions:
   - Click (**Approve**) next to the attestation case you want to approve.
   - Click (**Deny**) next to the attestation case you want to deny.

   TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
9. Click **Next**.
10. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
      - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
      - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
      - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
      - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

11. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363
- Multi-request resources (page description) on page 1394
- Multi-request resource (page description) on page 1395
- Attestation – Multi-request resource (page description) on page 1397

Sending reminders about multi-request resource pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the attestation case that has attestors you want to remind.
8. In the details pane, click **Actions** > **Send a reminder mail**.
9. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
10. Select the email program that you want to use.

This opens an email template with the attestor's email address.

11. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Send reminder**.
8. In the **Send a reminder mail** dialog, enter the message for the attestor.
9. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi-request resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
8. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- Multi-request resources (page description) on page 1394

- Multi-request resource (page description) on page 1395
- Attestation – Multi-request resource (page description) on page 1397

Managing multi requestable/unsubscribable resources

You can perform a variety of actions on multi requestable/unsubscribable resources and gather information about them.

Detailed information about this topic

- Displaying all multi requestable/unsubscribable resources on page 694
- Displaying multi requestable/unsubscribable resource overviews on page 695
- Displaying and editing multi requestable/unsubscribable resource main data on page 695
- Multi requestable/unsubscribable resource memberships on page 696
- Multi requestable/unsubscribable resource attestations on page 698

Displaying all multi requestable/unsubscribable resources

You can see all the multi requestable/unsubscribable resources.

To display multi requestable/unsubscribable resources

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.

   This opens the **Multi requestable/unsubscribable Resources** page (see Multi requestable/unsubscribable resources (page description) on page 1399) and displays all the multi requestable/unsubscribable resources.

Related topics

- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399

Displaying multi requestable/unsubscribable resource overviews

You can see all relevant information about multi requestable/unsubscribable resources summarized in an overview. The information is represented by shapes in a HyperView.

To display a multi requestable/unsubscribable resource's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <multi requestable/unsubscribable resource name>** page (see Overview – Multi requestable/unsubscribable resource (page description) on page 1401).

Related topics

- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399
- Multi requestable/unsubscribable resource (page description) on page 1399
- Overview – Multi requestable/unsubscribable resource (page description) on page 1401

Displaying and editing multi requestable/unsubscribable resource main data

You can see and edit multi requestable/unsubscribable resources' main data.

To show and edit a multi requestable/unsubscribable resource's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose main data you want to show/edit.
4. In the details pane, click **Edit**.
5. On the overview page, click **Main data**.

6. On the **Main data - <multi requestable/unsubscribable resource name>**, make your changes in the respective fields (see Main data – Multi requestable/unsubscribable resource (page description) on page 1401).
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399
- Multi requestable/unsubscribable resource (page description) on page 1399
- Main data – Multi requestable/unsubscribable resource (page description) on page 1401

Multi requestable/unsubscribable resource memberships

Multi requestable/unsubscribable resources can be assigned identities. You can see these identities, assign further identities to the multi requestable/unsubscribable resources and remove identities from the multi requestable/unsubscribable resources.

Detailed information about this topic

- Displaying multi requestable/unsubscribable resource memberships on page 696
- Assigning identities to multi requestable/unsubscribable resources on page 697
- Removing multi requestable/unsubscribable resources from identities on page 698

Displaying multi requestable/unsubscribable resource memberships

You can see identities that have multi requestable/unsubscribable resources assigned to them.

To display identities that are assigned a multi requestable/unsubscribable resource

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose memberships you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.

This opens the **Memberships - <multi requestable/unsubscribable resource name>** page (see Memberships – Multi requestable/unsubscribable resource (page description) on page 1402).

Related topics

- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399
- Multi requestable/unsubscribable resource (page description) on page 1399
- Memberships – Multi requestable/unsubscribable resource (page description) on page 1402

Assigning identities to multi requestable/unsubscribable resources

You can assign identities to multi requestable/unsubscribable resources. You do this through requests.

To assign a multi requestable/unsubscribable resource to an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resources you want to assign an identity to.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <multi requestable/unsubscribable resource name>** page, click **Request memberships**.
7. In the **Request memberships** dialog, in the list, click the identity you want to assign to the multi requestable/unsubscribable resource.
8. Click **Add to cart**.
9. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the multi requestable/unsubscribable resource.

Related topics

- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399
- Multi requestable/unsubscribable resource (page description) on page 1399
- Memberships – Multi requestable/unsubscribable resource (page description) on page 1402

Removing multi requestable/unsubscribable resources from identities

You can remove identities from multi requestable/unsubscribable resources

To remove an identity from a multi requestable/unsubscribable resource

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resources you want to remove an identity from.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <multi requestable/unsubscribable resource name>** page, select the check box next to the multi requestable/unsubscribable resource that you want to remove.
7. Click **Delete memberships**.

   This cancels the multi requestable/unsubscribable resource's assignment.

Related topics

- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399
- Multi requestable/unsubscribable resource (page description) on page 1399
- Memberships – Multi requestable/unsubscribable resource (page description) on page 1402

Multi requestable/unsubscribable resource attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager

attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying multi requestable/unsubscribable resource attestation cases on page 699
- Displaying attestors of multi requestable/unsubscribable resource pending attestation cases on page 700
- Approving and denying multi requestable/unsubscribable resource attestation cases on page 702
- Sending reminders about multi requestable/unsubscribable resource pending attestation cases on page 703

Displaying multi requestable/unsubscribable resource attestation cases

You can see attestation cases related to multi requestable/unsubscribable resources.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

This opens the **Attestation - <multi requestable/unsubscribable resource name>** page (see Attestation – Multi requestable/unsubscribable resource (page description) on page 1403).

6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click **Show details**.
    c. In the **Attested object** dialog, select an object in the **Object** menu.

       This shows information about the object.
    d. (Optional) Click **View current state of the object**

       This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
    a. In the list, click the attestation case.
    b. In the details pane, click the **History** tab.

       This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399
- Multi requestable/unsubscribable resource (page description) on page 1399
- Attestation – Multi requestable/unsubscribable resource (page description) on page 1403

Displaying attestors of multi requestable/unsubscribable resource pending attestation cases

You can see identities that still have to approve multi requestable/unsubscribable resource attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399
- Multi requestable/unsubscribable resource (page description) on page 1399
- Attestation – Multi requestable/unsubscribable resource (page description) on page 1403

Approving and denying multi requestable/unsubscribable resource attestation cases

You can grant or deny approval to attestation cases of multi requestable/unsubscribable resources.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to decide approval on.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Approve**.
8. On the **Attestation - <multi requestable/unsubscribable resource name>** page, perform one of the following actions:
    - Click (**Approve**) next to the attestation case you want to approve.
    - Click (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
9. Click **Next**.
10. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.

- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

11. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399
- Multi requestable/unsubscribable resource (page description) on page 1399
- Attestation – Multi requestable/unsubscribable resource (page description) on page 1403

Sending reminders about multi requestable/unsubscribable resource pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

6. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the attestation case that has attestors you want to remind.
8. In the details pane, click **Actions** > **Send a reminder mail**.
9. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
10. Select the email program that you want to use.

    This opens an email template with the attestor's email address.
11. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Send reminder**.
8. In the **Send a reminder mail** dialog, enter the message for the attestor.
9. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <multi requestable/unsubscribable resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.

8. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- Multi requestable/unsubscribable resources (page description) on page 1399
- Multi requestable/unsubscribable resource (page description) on page 1399
- Attestation – Multi requestable/unsubscribable resource (page description) on page 1403

Managing resources

You can perform a variety of actions on resources and gather information about them.

Detailed information about this topic

- Displaying all resources on page 705
- Displaying resource overviews on page 706
- Displaying and editing resource main data on page 706
- Resources' memberships on page 707
- Resource attestations on page 709
- Displaying role memberships resource members on page 715

Displaying all resources

You can see all the resources.

To display resources

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.

   This opens the **Resources** page (see Resources (page description) on page 1444) and displays all the resources.

Related topics

- Governance administration (page description) on page 1363
- Resources (page description) on page 1444

Displaying resource overviews

You can see all relevant information about resources summarized in an overview. The information is represented by shapes in a HyperView.

To display a resource's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <resource name>** page (see Overview – Resource (page description) on page 1446).

Related topics

- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Overview – Resource (page description) on page 1446

Displaying and editing resource main data

You can see and edit resources' main data.

To show and edit a resource's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose main data you want to show/edit.
4. In the details pane, click **Edit**.
5. On the overview page, click **Main data**.
6. On the **Main data - <resource name>**, make your changes in the respective fields (see Main data – Resource (page description) on page 1446).
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Main data – Resource (page description) on page 1446

Resources' memberships

Resources can be assigned identities. You can see these identities, assign further identities to the resources and remove identities from the resources.

Detailed information about this topic

- Displaying resource memberships on page 707
- Assigning identities to resources on page 707
- Removing resources from identities on page 708

Displaying resource memberships

You can see identities that have resources assigned to them.

To display identities that are assigned a resource

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose memberships you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <resource name>** page (see Memberships – Resource (page description) on page 1447).

Related topics

- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Memberships – Resource (page description) on page 1447

Assigning identities to resources

You can assign resources to identities. You do this through requests.

To assign a resource to an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource you want to assign an identity to.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <resource name>** page, click **Request memberships**.
7. In the **Request memberships** dialog, in the list, click the identity you want to assign to the resource.
8. Click **Add to cart**.
9. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the resource.

Related topics

- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Memberships – Resource (page description) on page 1447

Removing resources from identities

You can remove identities from resources.

To remove an identity from a resource

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource you want to remove an identity from.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <resource name>** page, select the check box next to the resource that you want to remove.
7. Click **Delete memberships**.

   This cancels the resource's assignment.

Related topics

- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Memberships – Resource (page description) on page 1447

Resource attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying resource attestation cases on page 709
- Displaying attestors of resource pending attestation cases on page 711
- Approving and denying resource attestation cases on page 712
- Sending reminders about resource pending attestation cases on page 713

Displaying resource attestation cases

You can see attestation cases related to resources.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <resource name>** page (see Attestation - Resource (page description) on page 1448).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Attestation - Resource (page description) on page 1448

Displaying attestors of resource pending attestation cases

You can see identities that still have to approve resource attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Attestation - Resource (page description) on page 1448

Approving and denying resource attestation cases

You can grant or deny approval to attestation cases of resources.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to decide approval on.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Approve**.
8. On the **Attestation - <resource name>** page, perform one of the following actions:
    - Click (**Approve**) next to the attestation case you want to approve.
    - Click (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
9. Click **Next**.
10. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
11. Click **Save**.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Attestation - Resource (page description) on page 1448

Sending reminders about resource pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the attestation case that has attestors you want to remind.
8. In the details pane, click **Actions** > **Send a reminder mail**.
9. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
10. Select the email program that you want to use.

    This opens an email template with the attestor's email address.
11. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Send reminder**.
8. In the **Send a reminder mail** dialog, enter the message for the attestor.
9. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
8. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Attestation - Resource (page description) on page 1448

Displaying role memberships resource members

. You can see which roles and organizations belong to identities that are assigned resources. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a resource

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Resources**.
3. On the **Resources** page, click the resource whose members you want to know more about.
4. In the details pane, click **Edit**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <resource name>** page (see Usage – Resource (page description) on page 1450).
6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Governance administration (page description) on page 1363
- Resources (page description) on page 1444
- Resource (page description) on page 1444
- Usage – Resource (page description) on page 1450

Managing locations

You can perform a variety of actions on locations and gather information about them.

Detailed information about this topic

- Displaying all locations on page 716
- Restoring deleted locations on page 716
- Displaying location overviews on page 717
- Displaying and editing location main data on page 718

Displaying all locations

You can see all the locations.

To display locations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.

   This opens the **Organization** page (see Organization (page description) on page 1405) and displays all the locations.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405

Restoring deleted locations

You can restore deleted locations. For example, a location can be deleted if two roles are merged during comparison (see Comparing and merging locations on page 739).

To restore a deleted location

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Organization** page, click **Restore a deleted role**.

4. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the location was deleted.
5. Next to the location you want to restore, select the check box.
6. Click **Next**.
7. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
8. Click **Next**.
9. Click **Close**.

To restore a deleted child location

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Organization** page, click the location that was originally parent to the deleted location.
4. In the details pane, click **Edit**.
5. On the overview page, click **Restore**.
6. In the **Restore a deleted role** dialog, in the date field next to **Find roles deleted from**, enter a date and time before the location was deleted.
7. In the list next to the location you want to restore, select the check box.
8. Click **Next**.
9. (Optional) To prevent certain actions from being performed, clear the check box next to the corresponding action.
10. Click **Next**.
11. Click **Close**.

Related topics

- Comparing and merging locations on page 739
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431

Displaying location overviews

You can see all relevant information about locations summarized in an overview. The information is represented by shapes in a HyperView.

To display a location's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Organization** page, click the location whose overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Overview**.

    This opens the **Overview - <location name>** page (see Overview - Location (page description) on page 1434).

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Overview - Location (page description) on page 1434

Displaying and editing location main data

You can see and edit locations' main data.

To show and edit a location's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Organization** page, click the location whose main data you want to display/edit.
4. In the details pane, click **Edit**.
5. On the overview page, click **Main data**.
6. On the **Main data - <location name>**, make your changes in the respective fields (see Main data - Location (page description) on page 1434).
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Main data - Location (page description) on page 1434

Location memberships

Identities can be assigned to locations. You can see these identities, assign further identities to the locations and remove identities from the locations.

Detailed information about this topic

- Displaying location memberships on page 719
- Assigning identities to locations on page 720
- Removing identities from locations on page 720

Displaying location memberships

You can see identities that have locations assigned to them.

To display identities that are assigned a location

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose memberships you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <location name>** page (see Memberships – Location (page description) on page 1435).

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Memberships – Location (page description) on page 1435

Assigning identities to locations

You can assign locations to identities. You do this through requests.

To assign an application role to an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location you want to assign an identity to.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <location name>** page, click **Request memberships**.
7. In the **Request memberships** dialog, in the list, click the identity you want to assign to the location.
8. Click **Add to cart**.
9. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    Once the request has been granted approval, the identity is assigned to the location.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Memberships – Location (page description) on page 1435

Removing identities from locations

You can remove identities from locations.

To remove an identity from a location

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location you want to remove an identity from.

4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <location name>** page, select the check box next to the location that you want to remove.
7. Click **Delete memberships**.

   This cancels the location's assignment.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Memberships – Location (page description) on page 1435

Location entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to locations you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the locations.

Detailed information about this topic

- Displaying location entitlements on page 721
- Adding location entitlements on page 722
- Deleting entitlements from locations on page 723

Displaying location entitlements

You can see entitlements assigned to locations. You can also display the reason why locations have certain entitlements (entitlement origin).

To display a location's entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose entitlements you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.

This opens the **Entitlements - <location name>** page (see Entitlements – Location (page description) on page 1436).

6. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Entitlements – Location (page description) on page 1436

Adding location entitlements

You can add entitlements to locations. You do this through a request.

To add an entitlement to a location

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location to which you want to add an entitlement.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.
6. On the **Entitlements - <location name>** page, click **Add new**.
7. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
8. Click **Assign**.
9. In the **Entitlement** dialog, in the list, click the entitlement that you want to add.
10. In the **Add a new entitlement** dialog, click **Request**.
11. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    After the request has been granted approval, the entitlement is added to the location.

Related topics

- Requesting products on page 86
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Entitlements – Location (page description) on page 1436
- My shopping cart (page description) on page 869

Deleting entitlements from locations

You can delete entitlements assigned to locations.

To delete an entitlement of a location

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose entitlements you want to delete.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.
6. On the **Entitlements - <location name>** page, in the list, select the check box in the row of the entitlement you want to delete.
7. Click **Delete**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Entitlements – Location (page description) on page 1436

Compliance: Locations

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity's Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying location rule violations on page 724
- Displaying location policy violations on page 725
- Displaying rule violations of location members on page 725
- Displaying risk indexes and entitlements of location members on page 726

Displaying location rule violations

You can see location rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance**.

   This opens the **Compliance - <location name>** page (see Compliance – Location (page description) on page 1437).

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Compliance – Location (page description) on page 1437

Displaying location policy violations

You can see location policy violations.

To display policy violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose policy violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <location name>** page (see Compliance reports - Location (page description) on page 1443).
6. In the **View** menu, select **Policy violations**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Compliance reports - Location (page description) on page 1443

Displaying rule violations of location members

You can see the rule violations of identities that are assigned specific locations.

To display rule violations of a location's members

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:

    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <location name>** page (see Compliance reports - Location (page description) on page 1443).
6. In the **View** menu, select **Compliance rule violations**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Compliance reports - Location (page description) on page 1443

Displaying risk indexes and entitlements of location members

For every location, you can see all the identities that have this location as primary or secondary assignment. You can also display the number of entitlements assigned and the risk index.

To display members of a location

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose members you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <location name>** page (see Compliance reports - Location (page description) on page 1443).
6. In the **View** menu, select **Identities: Risk indexes and entitlements**.
7. (Optional) To display more information about an identity, perform the following actions:
    a. In the list, click an identity.
    b. In the dialog, click **Overview**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Compliance reports - Location (page description) on page 1443

Location attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying location attestation cases on page 727
- Displaying attestors of location pending attestation cases on page 729
- Approving and denying location attestation cases on page 730
- Sending reminders about location pending attestation cases on page 731

Displaying location attestation cases

You can see attestation cases related to locations.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <location name>** page (see Attestation – Location (page description) on page 1438).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Attestation – Location (page description) on page 1438

Displaying attestors of location pending attestation cases

You can see identities that still have to approve location attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363

- Organization (page description) on page 1405
- Location (page description) on page 1431
- Attestation – Location (page description) on page 1438

Approving and denying location attestation cases

You can grant or deny approval to attestation cases of locations.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose attestation cases you want to decide approval on.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Approve**.
8. On the **Attestation - <location name>** page, perform one of the following actions:
    - Click ☑ (**Approve**) next to the attestation case you want to approve.
    - Click ☒ (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
9. Click **Next**.
10. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.

- To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.

- To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

11. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Attestation – Location (page description) on page 1438

Sending reminders about location pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose attestation cases you want to display.
4. In the details pane, click **Edit**.

5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the attestation case that has attestors you want to remind.
8. In the details pane, click **Actions** > **Send a reminder mail**.
9. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
10. Select the email program that you want to use.

    This opens an email template with the attestor's email address.
11. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Send reminder**.
8. In the **Send a reminder mail** dialog, enter the message for the attestor.
9. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <location name>** page, click on a tab to display the corresponding attestation cases.

7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
8. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Attestation – Location (page description) on page 1438

Displaying location risk indexes

You can see location risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a cost center's risk index

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose risk index you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Risk**.

   This opens the **Risk - <location name>** page (see Risk – Location (page description) on page 1111).
6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- Risk assessment on page 209
- Governance administration (page description) on page 1363

- Organization (page description) on page 1405
- Location (page description) on page 1431
- Overview - Location (page description) on page 1434

Location history

The Web Portal gives you the option of displaying the historical data of locations for which you are responsible.

To do this, you have the following options:

Table 51: Historical data

View	Description
Events	This shows you all the events that affect the location, either on a timeline or in a table (see Displaying location history on page 734).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of locations on page 735).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of locations on page 736).

Displaying location history

You can select to display all events involving locations on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose history you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

This opens the **History - <location name>** page (see History – Location (page description) on page 1440).

> TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
>
> To zoom in or out, turn the mouse wheel.

6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
    - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
    - **Change type**: Only show events on the timeline with the selected change type.
    - **Date**: Only show events on the timeline that took place in the given period.
    - **Properties**: Only show events on the timeline with the selected properties.
    - **Display**: Only show events on the timeline that match the search.
    - **Object**: Only show events on the timeline about the selected object.
7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
    - Click on the event in the timeline.
    - In the table view, click the event and you will see the details in the details pane.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- History – Location (page description) on page 1440

Displaying the status overview of locations

You can see all the changes that affect locations. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:

a. Click **Organization**.

b. On the **Organization** page, click **Locations** in the **Type** drop-down.

3. On the **Locations** page, click the location whose status overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

   This opens the **History - <location name>** page (see History – Location (page description) on page 1440).
6. Click the **Status overview** tab.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- History – Location (page description) on page 1440

Comparing statuses of locations

You can compare the current status of a location that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.
6. On the **History** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:

a. Click **Organization**.

b. On the **Organization** page, click **Locations** in the **Type** drop-down.

3. On the **Locations** page, click the location whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.
6. On the **History** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
7. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- History – Location (page description) on page 1440

Displaying role memberships of location members

. You can see which roles and organizations belong to identities that are assigned locations. Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a location

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location whose members you want to know more about.
4. In the details pane, click **Edit**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <location name>** page (see Usage – Location (page description) on page 1442).

6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click ⓘ (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431
- Usage – Location (page description) on page 1442

Copying/splitting locations

You can copy or move memberships and entitlements from location to new roles (departments, business roles, cost centers, locations).

Any combination of role types is allowed.

To copy a location or move memberships and entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location you want to copy or whose memberships and entitlements you want to move.
4. In the details pane, click **Edit**.
5. On the overview page, click **Split**.
6. In the **Split a role** dialog, in the **Type of the new role** menu, select a type for the new role.
7. Depending on which role type you have selected, enter the corresponding main data of the new role (see Main data – Department (page description) on page 1079, Main data – Business role (page description) on page 1050, Main data – Cost center (page description) on page 1093, or Main data - Location (page description) on page 1106).
8. Click **Next**.
9. Perform the following actions:
   - To neither copy nor move a entitlement/membership to a new role, click **Actions** > **Keep this assignment** next to the corresponding entitlement/membership. Later, the entitlement/membership is only available

in the source role.

- To copy a entitlement/membership to a new role, click **Actions** > **Keep and copy to new role** next to the corresponding entitlement/membership. The entitlement/membership is later included in the source role as well as the target role.
- To move a entitlement/membership to a new role, click **Actions** > **Move to new role** next to the corresponding entitlement/membership. The entitlement/membership is later removed from the source role and is only included in the target role.

10. Click **Next**.
11. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
12. Click **Next**.
13. Click **Close**.

Related topics

- Location memberships on page 719
- Location entitlements on page 721
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431

Comparing and merging locations

You can compare the properties of locations with the properties of other business roles, departments, cost centers, or locations and then select the properties you require and merge them.

To compare and merge a location

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
    a. Click **Organization**.
    b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Locations** page, click the location you want to compare and merge.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compare and merge**.
6. In the **Compare and merge** dialog, in the **Object type** menu, select the business role, department, cost center, or location to compare and merge with your location.

7. Click **Assign**.
8. In the **Comparison role** dialog, select the business role/department/cost center/location to compare.

   The assigned memberships and entitlements of both objects are listed with the following information:

   Table 52: Overview of the assignments

Column	Description
Object	Shows the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.
Type	Type of the entitlement/membership.
<Name of the source object>	Shows the entitlement/membership's assignment type. The following assignment types are available. • Direct • Inherited • Requested • Dynamic • Not assigned For more detailed information about assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.
<Name of the compare object>	
Comparison	Show you where the entitlement/membership occurs.

   TIP: To arrange the list of assignments better, use the filters available some of the columns. For more information, see Filtering on page 40..

9. In the **Compare and merge** dialog, click **Merge the selected roles**.
10. (Optional) Verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.
12. Click **Close**.

Related topics

- Location memberships on page 719
- Location entitlements on page 721
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431

Displaying location statistics

You can see location statistics.

To display a location's statistics

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, perform the following actions:
   a. Click **Organization**.
   b. On the **Organization** page, click **Locations** in the **Type** drop-down.
3. On the **Organization** page, click the location whose statistics you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Statistics**.

   This opens the **Statistics for <location name>** dialog and shows the location's statistics.
6. (Optional) To obtain more information about a chart, click the chart or its header.

Related topics

- Discovering your statistics on the home page on page 795
- Statistics on page 795
- Governance administration (page description) on page 1363
- Organization (page description) on page 1405
- Location (page description) on page 1431

System entitlements

System entitlements map the objects that control access to target system resources in the target systems. A user account obtains the required permissions for accessing target system resources through its memberships in system entitlements.

You can perform a variety of actions on system entitlements and gather information about them.

Detailed information about this topic

- Displaying all system entitlements on page 742
- Displaying system entitlement overviews on page 742
- Displaying and editing system entitlements main data on page 743
- System entitlement memberships on page 745

- System entitlement attestations on page 749
- System entitlement product owners on page 756
- System entitlement history on page 759
- Displaying role memberships of system entitlement members on page 762

Displaying all system entitlements

You can see all the system entitlements.

To display system entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.

   This opens the **System Entitlements** page (see System entitlements (page description) on page 1450) and displays all the system entitlements.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450

Displaying system entitlement overviews

You can see all relevant information about system entitlements summarized in an overview. The information is represented by shapes in a HyperView.

To display a system entitlement's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose overview you want to display.
4. On the overview page, click **Overview**.

   This opens the **Overview - <system entitlement name>** page (see Overview – System entitlement (page description) on page 1453).

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Overview – System entitlement (page description) on page 1453

Displaying and editing system entitlements main data

You can see and edit system entitlements' main data.

To show and edit a system entitlement's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose main data you want to display/edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <system entitlement name>**, make your changes in the respective fields (see Main data – System entitlement (page description) on page 1453).
6. Click **Save**.

To edit the group scope and group type of an Active Directory group

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the Active Directory that you want to edit.
4. On the overview page, click **Main data**.
5. On the **Main data - <Active Directory group name>**, click **Request modification**.
6. In the **Modify Active Directory group** dialog, make your changes in the respective fields:
    - **Group scope**: Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can specify one of the following group scopes:
        - **Global group**: Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group’s domain.
        - **Local**: Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.
        - **Universal**: Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
    - **Group type**: Specify whether this is an Active Directory security group or an Active Directory distribution group.

7. Click **OK**.
8. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    The Active Directory group changes after the modifications to the Active Directory group have been granted approval.

Related topics

- Requesting products on page 86
- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Main data – System entitlement (page description) on page 1453
- My shopping cart (page description) on page 869

Deleting Active Directory groups

You cannot delete Active Directory groups directly. You can request deletion of the Active Directory groups and await approval of the request.

To delete Active Directory groups

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the Active Directory group that you want to delete.
4. On the overview page, click **Main data**.
5. On the **Main data - <Active Directory group name>**, click **Request deletion**.
6. In the dialog, confirm the prompt with **Yes**.
7. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    The Active Directory group is deleted after it has been granted approval.

Related topics

- Requesting products on page 86
- Governance administration (page description) on page 1363

- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Main data – System entitlement (page description) on page 1453
- My shopping cart (page description) on page 869

System entitlement memberships

System entitlements can be assigned identities. You can see these identities, assign further identities to the system entitlements and remove identities from the system entitlements.

Detailed information about this topic

- Displaying system entitlement memberships on page 745
- Assigning identity system entitlements on page 745
- Removing system entitlements from identities on page 746

Displaying system entitlement memberships

You can see identities that have system entitlements assigned to them.

To display identities that are assigned a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose memberships you want to display.
4. On the overview page, click **Memberships**.

   This opens the **Memberships - <system entitlement name>** page (see Memberships – System entitlement (page description) on page 1455).

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Memberships – System entitlement (page description) on page 1455

Assigning identity system entitlements

You can assign system entitlements to identities. You do this through requests.

To assign a system entitlement to an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement you want to assign to an identity.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <system entitlement name>** page, click **Request memberships**.
6. In the **Request memberships** dialog, in the list, click the identity you want to assign to the system entitlement.
7. Click **Add to cart**.
8. On the **My Shopping Cart** page, click **Submit**.

   > TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the system entitlement.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Memberships – System entitlement (page description) on page 1455

Removing system entitlements from identities

You can remove identities from system entitlements.

To remove an identity from a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement you want to remove an identity from.
4. On the overview page, click **Memberships**.
5. On the **Memberships - <system entitlement name>** page, select the check box next to the system entitlements that you want to remove.
6. Click **Delete memberships**.

   This cancels the system entitlement's assignment.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Memberships – System entitlement (page description) on page 1455

System entitlements' child groups

You can order more groups under certain group types or order these under other groups:

- Active Directory groups
- LDAP groups
- Notes groups
- Custom target systems groups

Detailed information about this topic

- Displaying system entitlements' child groups on page 747
- Assigning child groups to system entitlements on page 748
- Removing system entitlements' child groups on page 748

Displaying system entitlements' child groups

You can see child groups of system entitlements.

To display the child groups of a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose child groups you want to display.
4. On the overview page, click **Child groups**.

   This opens the **Child groups - <system entitlement name>** page (see Child groups – System entitlement (page description) on page 1038).

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Child groups – System entitlement (page description) on page 1456

Assigning child groups to system entitlements

You can assign child groups to system entitlements

To assign a child group to a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement you want to assign a child group to.
4. On the overview page, click **Child groups**.
5. On the **Child groups - <system entitlement name>**, click **New child group**.
6. In the **Add members group** dialog, click **Assign**.
7. In the **Child group** dialog, in the list, click the group you want to add to the system entitlement.
8. In the **Add members group** dialog, click **Save**.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Child groups – System entitlement (page description) on page 1456

Removing system entitlements' child groups

You can remove child groups of system entitlements.

To remove a child group from a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose child groups you want to remove.
4. On the overview page, click **Child groups**.
5. On the **Child groups - <system entitlement name>** page, in the list, select the check box in the row of the child group that you want to remove.
6. Click **Remove selected**.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Child groups – System entitlement (page description) on page 1456

System entitlement attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying system entitlement attestation cases on page 749
- Displaying attestors of system entitlement pending attestation cases on page 750
- Approving and denying system entitlement attestation cases on page 751
- Sending reminders about system entitlement pending attestation cases on page 753

Displaying system entitlement attestation cases

You can see attestation cases related to system entitlements.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.

   This opens the **Attestation - <system entitlement name>** page (see Attestation – System entitlement (page description) on page 1457).
5. (Optional) Click on a tab to display the respective attestation cases.
6. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
7. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
8. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Attestation – System entitlement (page description) on page 1457

Displaying attestors of system entitlement pending attestation cases

You can see identities that still have to approve system entitlement attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
6. In the list, click the (pending) attestation case that has attestors you want to display.
7. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
6. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Attestation – System entitlement (page description) on page 1457

Approving and denying system entitlement attestation cases

You can grant or deny approval to attestation cases of system entitlements.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to decide approval on.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
6. Click **Approve**.
7. On the **Pending Attestations - <system entitlement name>** page, perform one of the following actions:
    - Click (**Approve**) next to the attestation case you want to approve.
    - Click (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
8. Click **Next**.
9. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
10. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363

- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Attestation – System entitlement (page description) on page 1457

Sending reminders about system entitlement pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
6. In the list, click the attestation case that has attestors you want to remind.
7. In the details pane, click **Actions** > **Send a reminder mail**.
8. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
9. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
10. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
6. Click **Send reminder**.
7. In the **Send a reminder mail** dialog, enter the message for the attestor.
8. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. On the overview page, click **Attestation**.
5. (Optional) On the **Attestations – <system entitlement name>** page, click on a tab to display the corresponding attestation cases
6. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
7. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
8. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Attestation – System entitlement (page description) on page 1457

System entitlements' attestors

Identities that can approve attestation cases of system entitlements are assigned as attestors through application roles.

Detailed information about this topic

- Displaying system entitlement attestors on page 755
- Specifying attestors of system entitlements on page 755

Displaying system entitlement attestors

You can display which identities can attest system entitlements.

To display attestors of a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestor you want to display.
4. On the overview page, click **Attestors**.

   This opens the **Attestors - <system entitlement name>** page (see Attestors – System entitlement (page description) on page 1459). In the details pane, under **Assigned**, all the identities to which the assigned application role is assigned are displayed. These identities can approve system entitlement attestation cases.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Attestors – System entitlement (page description) on page 1459

Specifying attestors of system entitlements

You can specify identities that can approve system entitlement attestation cases.

To specify attestors for a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestor you want to specify.
4. On the overview page, click **Attestors**.
5. On the **Attestors - <system entitlement name>** page, perform one of the following actions:

a. Next to **Attestor**, click **Assign/Change**.

b. In the **Attestors** dialog, click an application role in the list whose members can approve the system entitlement's attestation cases.

6. (Optional) To assign additional identities to the application role so that those identities can approve the system entitlement attestation case, click the appropriate identities in the list.
7. Click **Save**.

To create a new attestor role for a system entitlement and assign it.

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestor you want to specify.
4. On the overview page, click **Attestors**.
5. On the **Attestors - <system entitlement name>** page, click **Add new**.
6. In the **Create new attestor application role** dialog, enter additional information about the new application role:
   - **Application role**: Enter a name for the new application role.
   - **Description**: (Optional) Enter a description for the new application role.
7. Click **Save**.
8. On the **Attestors - <name of system entitlement>** page, in the list, click the identities that can approve the system entitlement's attestation cases. This assigns the identities to the application role.
9. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Attestors – System entitlement (page description) on page 1459

System entitlement product owners

Identities responsible for system entitlements are assigned as owners through application roles.

Detailed information about this topic

- Displaying product owners of system entitlements on page 757
- Specifying product owners for system entitlements on page 757

Displaying product owners of system entitlements

You can display identities that are responsible for system entitlements .

To display the owners of a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose owners you want to display.
4. On the overview page click **Owners**.

   This opens the **Owners - <system entitlement name>** page (see Owners – System entitlement (page description) on page 1459). In the details pane, under **Assigned**, all the identities to which the assigned application role is assigned are displayed. These identities are responsible for the system entitlement.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Owners – System entitlement (page description) on page 1459

Specifying product owners for system entitlements

You can specify which identities are responsible for system entitlements.

To specify owners for a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose product owner you want to specify.
4. On the overview page click **Owners**.
5. On the **Owners - <system entitlement name>** page, perform one of the following actions:

   a. Next to **Product owner**, click **Assign**/**Change**.
   b. In the **Product owner** dialog, in the list, click an application role whose members are responsible for the system entitlement.
6. (Optional) To assign the application role to additional identities so that those identities are responsible for system entitlement, click the appropriate identities in the list.
7. Click **Save**.

To create and assign a new owner role for a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose owners you want to specify.
4. On the overview page click **Owners**.
5. On the **Owners - <system entitlement name>** page, click **Add new**.
6. In the **Create new owner role** dialog, enter additional information about the new application role:
   - **Application role**: Enter a name for the new application role.
   - **Description**: (Optional) Enter a description for the new application role.
7. Click **Save**.
8. On the **Owners - <system entitlement name>** page, in the list, click the identities that will be responsible for the system entitlement. This assigns the identities to the application role.
9. Click **Save**.

To create and assign a new owner role with the same members as the currently selected owner role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose owners you want to specify.
4. On the overview page click **Owners**.
5. On the **Owners - <system entitlement name>** page, click **Move ownership**.
6. In the **Move ownership to new owner role** dialog, select the check box next to **Move all owners**.
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- Owners – System entitlement (page description) on page 1459

System entitlement history

The Web Portal gives you the option of displaying the historical data of system entitlements for which you are responsible.

To do this, you have the following options:

Table 53: Historical data

View	Description
Events	This shows you all the events that affect the system entitlement, either on a timeline or in a table (see Displaying system entitlement history on page 759).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of system entitlements on page 760).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of system entitlements on page 761).

Displaying system entitlement history

You can select to display all events involving system entitlements on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose history you want to display.
4. On the overview page, click **History**.

This opens the **History - <system entitlement name>** page (see History – System entitlement (page description) on page 1460).

TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

To zoom in or out, turn the mouse wheel.

5. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
6. (Optional) To switch to the table view, click **Switch to table view**.
7. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- History – System entitlement (page description) on page 1460

Displaying the status overview of system entitlements

You can see all the changes that affect system entitlements. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose status overview you want to display.
4. On the overview page, click **History**.

   This opens the **History - <system entitlement name>** page (see History – System entitlement (page description) on page 1460).
5. Click the **Status overview** tab.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- History – System entitlement (page description) on page 1460

Comparing statuses of system entitlements

You can compare the current status of a system entitlement that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, click the **Status comparison** tab.
6. In the date field, select the date and time from which you want to start the comparison.
7. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose status you want to compare.
4. On the overview page, click **History**.
5. On the **History** page, perform one of the following actions:

- On the timeline, click the event and then **Compare**.
- In the table view, click the event in the list and then in the details pane, click **Compare**.

6. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450
- System entitlement (page description) on page 1451
- History – System entitlement (page description) on page 1460

Displaying role memberships of system entitlement members

You can see which roles and organizations belong to identities that are assigned system entitlements. . Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a system entitlement

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose members you want to know more about.
4. On the overview page, click **Usage**.

   This opens the **Usage - <system entitlement name>** page (see Usage – System entitlement (page description) on page 1463).
5. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
6. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
7. (Optional) To see the legend, click **More information**.

Related topics

- Governance administration (page description) on page 1363
- System entitlements (page description) on page 1450

- System entitlement (page description) on page 1451
- Usage – System entitlement (page description) on page 1463

Managing system roles

You can perform a variety of actions on system roles and gather information about them.

Detailed information about this topic

- Displaying all system roles on page 763
- Displaying system role overviews on page 764
- Displaying and editing system role main data on page 764
- System role memberships on page 765
- System role entitlements on page 767
- Compliance: System roles on page 769
- System role attestations on page 772
- Displaying system role risk indexes on page 778
- System role history on page 779
- Displaying role memberships of system role members on page 782

Displaying all system roles

You can see all the system roles.

To display system roles

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.

   This opens the **System Roles** page (see System roles (page description) on page 1463) and displays all the system roles.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463

Displaying system role overviews

You can see all relevant information about system roles summarized in an overview. The information is represented by shapes in a HyperView.

To display a system role's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <system role name>** page (see Overview – System role (page description) on page 1466).

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Overview – System role (page description) on page 1466

Displaying and editing system role main data

You can see and edit the business roles' main data.

To show and edit a system role's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose main data you want to display/edit.
4. In the details pane, click **Edit**.
5. On the overview page, click **Main data**.
6. On the **Main data - <system role name>**, make your changes in the respective fields (see Main data – System role (page description) on page 1466).
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Main data – System role (page description) on page 1466

System role memberships

System roles can be assigned identities. You can see these identities, assign further identities to the system roles and remove identities from the system roles.

Detailed information about this topic

- Displaying system role memberships on page 765
- Assigning identities to system roles on page 766
- Removing identities from my system roles on page 766

Displaying system role memberships

You can see identities that have system roles assigned to them.

To display identities that are assigned a system role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose memberships you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.

   This opens the **Memberships - <system role name>** page (see Memberships – System role (page description) on page 1467).

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Memberships – System role (page description) on page 1467

Assigning identities to system roles

You can assign system roles to identities. You do this through requests.

To assign a system role to an identity

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role you want to assign to an identity.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.
6. On the **Memberships - <system role name>** page, click **Request memberships**.
7. In the **Request memberships** dialog, in the list, click the identity you want to assign to the system role.
8. Click **Add to cart**.
9. On the **My Shopping Cart** page, click **Submit**.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

   Once the request has been granted approval, the identity is assigned to the system role.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Memberships – System role (page description) on page 1467

Removing identities from my system roles

You can remove identities from system roles.

To remove an identity from a system role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role you want to remove an identity from.
4. In the details pane, click **Edit**.
5. On the overview page, click **Memberships**.

6. On the **Memberships - <system role name>** page, select the check box next to the system role that you want to remove.
7. Click **Delete memberships**.

   This cancels the system role's assignment.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Memberships – System role (page description) on page 1467

System role entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. Assigning identities to system roles avoids you having to assign entitlements separately to each identity. All a system role's entitlements are automatically assigned to all the identities assigned to the system role.

Detailed information about this topic

- Displaying system role entitlements on page 767
- Adding system role entitlements on page 768
- Deleting system role entitlements on page 769

Displaying system role entitlements

You can see entitlements assigned to system roles. You can also display the reason why system roles have certain entitlements (entitlement origin).

To display a system role's entitlements

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose entitlements you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.

   This opens the **Entitlements - <system role name>** page (see Entitlements – System role (page description) on page 1468).

6. (Optional) To display more information about the origin of an entitlement, perform the following actions:
   a. In the list, click the entitlement that you want to know more about.
   b. In the details pane, on the **Detective** tab, click ▶ (**Expand**) next to **Analysis for**.

      This displays more information about the entitlement's assignment.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Entitlements – System role (page description) on page 1468

Adding system role entitlements

You can add entitlements to system roles. You do this through a request.

To add an entitlement to a system role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role to which you want to add an entitlement.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.
6. On the **Entitlements - <system role name>** page, click **Add new**.
7. In the **Add a new entitlement** dialog, in the **Entitlement type** menu, select which type of entitlement you want to add.
8. Click **Assign**.
9. In the **Entitlement** dialog, in the list, click the entitlement that you want to add.
10. In the **Add a new entitlement** dialog, click **Request**.
11. On the **My Shopping Cart** page, click **Submit**.

    TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 88.

    After the request has been granted approval, the entitlement is added to the system role.

Related topics

- Requesting products on page 86
- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Entitlements – System role (page description) on page 1468
- My shopping cart (page description) on page 869

Deleting system role entitlements

You can delete entitlements assigned to system roles.

To delete an entitlement of a system role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose entitlements you want to delete.
4. In the details pane, click **Edit**.
5. On the overview page, click **Entitlements**.
6. On the **Entitlements - <system role name>** page, in the list, select the check box in the row of the entitlement you want to delete.
7. Click **Delete**.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Entitlements – System role (page description) on page 1468

Compliance: System roles

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity's Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- Displaying system role rule violations on page 770
- Displaying system role policy violations on page 771
- Displaying rule violations of system role members on page 771
- Displaying risk indexes and entitlements of system role members on page 772

Displaying system role rule violations

You can see system role rule violations.

To display rule violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance**.

   This opens the **Compliance - <system role name>** page (see Compliance – System role (page description) on page 1469).

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463

- System role (page description) on page 1463
- Compliance – System role (page description) on page 1469

Displaying system role policy violations

You can see system role policy violations.

To display policy violations

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose policy violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <system role name>** page (see Compliance reports – system role (page description) on page 1475).
6. In the **View** menu, select **Policy violations**.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Compliance reports – system role (page description) on page 1475

Displaying rule violations of system role members

You can see the rule violations of identities that are assigned specific system roles.

To display rule violations of a system role's members

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose rule violations you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <system role name>** page (see Compliance reports – system role (page description) on page 1475).
6. In the **View** menu, select **Compliance rule violations**.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Compliance reports – system role (page description) on page 1475

Displaying risk indexes and entitlements of system role members

For every system role, you can see all the identities that have this system role as primary or secondary assignment. You can also display the number of entitlements assigned and the risk index.

To display members of a system role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose members you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Compliance reports**.

   This opens the **Compliance reports - <system role name>** page (see Compliance reports – system role (page description) on page 1475).
6. In the **View** menu, select **Identities: Risk indexes and entitlements**.
7. (Optional) To display more information about an identity, perform the following actions:
   a. In the list, click an identity.
   b. In the dialog, click **Overview**.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Compliance reports – system role (page description) on page 1475

System role attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager

attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying system role attestation cases on page 773
- Displaying attestors of system role pending attestation cases on page 774
- Approving and denying system role attestation cases on page 775
- Sending reminders about system role pending attestation cases on page 776

Displaying system role attestation cases

You can see attestation cases related to system roles.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <system role name>** page (see Attestation – System role (page description) on page 1470).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:

a. In the list, click the attestation case.
b. In the details pane, click **Show details**.
c. In the **Attested object** dialog, select an object in the **Object** menu.

   This shows information about the object.
d. (Optional) Click **View current state of the object**

   This opens an overview of the attestation.

8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Attestation – System role (page description) on page 1470

Displaying attestors of system role pending attestation cases

You can see identities that still have to approve system role attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the (pending) attestation case that has attestors you want to display.

8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Attestation – System role (page description) on page 1470

Approving and denying system role attestation cases

You can grant or deny approval to attestation cases of system roles.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to decide approval on.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
7. Click **Approve**.

8. On the **Pending Attestations - <system role name>** page, perform one of the following actions:
    - Click (**Approve**) next to the attestation case you want to approve.
    - Click (**Deny**) next to the attestation case you want to deny.

    TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
9. Click **Next**.
10. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
        - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
        - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
        - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

    NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
11. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Attestation – System role (page description) on page 1470

Sending reminders about system role pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
7. In the list, click the attestation case that has attestors you want to remind.
8. In the details pane, click **Actions** > **Send a reminder mail**.
9. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
10. Select the email program that you want to use.

    This opens an email template with the attestor's email address.
11. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
7. Click **Send reminder**.
8. In the **Send a reminder mail** dialog, enter the message for the attestor.
9. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <system role name>** page, click on a tab to display the corresponding attestation cases
7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
8. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Attestation – System role (page description) on page 1470

Displaying system role risk indexes

You can see system role risk indexes.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display a system role's risk index

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose risk index you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Risk**.

This opens the **Risk - <system role name>** page (see Risk – System role (page description) on page 1071).

6. (Optional) To show which attributes and assignments contribute to the calculated risk index, click **View risk functions**.

Related topics

- Risk assessment on page 209
- Risk assessment on page 209
- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Overview – System role (page description) on page 1466

System role history

The Web Portal gives you the option of displaying the historical data of system roles for which you are responsible.

To do this, you have the following options:

Table 54: Historical data

View	Description
Events	This shows you all the events that affect the system role, either on a timeline or in a table (see Displaying system role history on page 779).
Status overview	This shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of system roles on page 780).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of system roles on page 781).

Displaying system role history

You can select to display all events involving system roles on a timeline or in a table.

To display the history

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose history you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

   This opens the **History - <system role name>** page (see History – System role (page description) on page 1472).

   > TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   >
   > To zoom in or out, turn the mouse wheel.

6. (Optional) To filter the timeline of events, click **Filter by** and then one of the following:
   - **User**: Searches for events or actions associated with the identity name given. Identities with entitlements and ownerships create changes, such as adding or removing properties. You can see these actions on the timeline.
   - **Change type**: Only show events on the timeline with the selected change type.
   - **Date**: Only show events on the timeline that took place in the given period.
   - **Properties**: Only show events on the timeline with the selected properties.
   - **Display**: Only show events on the timeline that match the search.
   - **Object**: Only show events on the timeline about the selected object.
7. (Optional) To switch to the table view, click **Switch to table view**.
8. (Optional) To show more details about an event, perform one of the following actions:
   - Click on the event in the timeline.
   - In the table view, click the event and you will see the details in the details pane.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- History – System role (page description) on page 1472

Displaying the status overview of system roles

You can see all the changes that affect system roles. You can also display how long each change was valid for. Use the status overview to track when changes were made and by

whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose status overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.

   This opens the **History - <system role name>** page (see History – System role (page description) on page 1472).
6. Click the **Status overview** tab.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- History – System role (page description) on page 1472

Comparing statuses of system roles

You can compare the current status of a system role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.
6. On the **History** page, click the **Status comparison** tab.
7. In the date field, select the date and time from which you want to start the comparison.
8. (Optional) To display the properties that have not changed since creation,deselect the box next to **Display changed values only**.

To compare the current status with the status at the time of a specific event

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose status you want to compare.
4. In the details pane, click **Edit**.
5. On the overview page, click **History**.
6. On the **History** page, perform one of the following actions:
   - On the timeline, click the event and then **Compare**.
   - In the table view, click the event in the list and then in the details pane, click **Compare**.
7. (Optional) To display the properties that have not changed since being created, deselect the box next to **Display changed values only**.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- History – System role (page description) on page 1472

Displaying role memberships of system role members

You can see which roles and organizations belong to identities that are assigned system roles. . Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

MOBILE: This function is not available in the mobile interface.

To display roles and organizations of members of a system role

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **System Roles**.
3. On the **System Roles** page, click the system role whose members you want to know more about.
4. In the details pane, click **Edit**.
5. On the overview page, click **Usage**.

   This opens the **Usage - <system role name>** page (see Usage – System role (page description) on page 1474).

6. In the **Role classes** menu, select the main category of roles and organizations that you want to display.
7. (Optional) To find out which members are assigned to a particular object, click (**More information**) in the specified object.
8. (Optional) To see the legend, click **More information**.

Related topics

- Governance administration (page description) on page 1363
- System roles (page description) on page 1463
- System role (page description) on page 1463
- Usage – System role (page description) on page 1474

Managing assignment resources

Use assignment resources to request hierarchical roles, such as departments or business roles and assign them to identities, devices, and workdesks. For example, you can limit assignment resources to a certain business roles, which makes it unnecessary to select the business role additionally when you request an assignment resource. It is automatically a part of the assignment request.

You can perform a variety of actions on assignments resources and gather information about them.

Detailed information about this topic

- Displaying all assignment resources on page 783
- Displaying assignment resource overviews on page 784
- Displaying and editing assignment resource main data on page 784
- Assignment resource attestations on page 785

Displaying all assignment resources

You can see all the assignment resources.

To display assignment resources

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.

   This opens the **Assignment Resources** page (see Assignment resources (page description) on page 1476) and displays all the resources.

Related topics

- Governance administration (page description) on page 1363
- Assignment resources (page description) on page 1476

Displaying assignment resource overviews

You can see all relevant information about assignment resources summarized in an overview. The information is represented by shapes in a HyperView.

To display an assignment resource's overview

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose overview you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Overview**.

   This opens the **Overview - <assignment resource name>** page (see Overview – Assignment resource (page description) on page 1477).

Related topics

- Governance administration (page description) on page 1363
- Assignment resources (page description) on page 1476
- Assignment resource (page description) on page 1477
- Overview – Assignment resource (page description) on page 1477

Displaying and editing assignment resource main data

You can see and edit assignment resources' main data.

To show and edit an assignment resource's main data

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose main data you want to show/edit.
4. In the details pane, click **Edit**.
5. On the overview page, click **Main data**.

6. On the **Main data - <assignment resource name>**, make your changes in the respective fields (see Main data – Assignment resource (page description) on page 1478).
7. Click **Save**.

Related topics

- Governance administration (page description) on page 1363
- Assignment resources (page description) on page 1476
- Assignment resource (page description) on page 1477
- Main data – Assignment resource (page description) on page 1478

Assignment resource attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

Detailed information about this topic

- Displaying assignment resource attestation cases on page 785
- Displaying attestors of assignment resource pending attestation cases on page 787
- Approving and denying assignment resource attestation cases on page 788
- Sending reminders about assignment resource pending attestation cases on page 789

Displaying assignment resource attestation cases

You can see attestation cases related to assignment resources.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.

   This opens the **Attestation - <assignment resource name>** page (see Attestation - Assignment resource (page description) on page 1479).
6. (Optional) Click on a tab to display the respective attestation cases.
7. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click **Show details**.
   c. In the **Attested object** dialog, select an object in the **Object** menu.

      This shows information about the object.
   d. (Optional) Click **View current state of the object**

      This opens an overview of the attestation.
8. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **Workflow** tab.
9. (Optional) To show previous attestation cases for the selected object, perform the following actions:
   a. In the list, click the attestation case.
   b. In the details pane, click the **History** tab.

      This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Related topics

- Governance administration (page description) on page 1363
- Assignment resources (page description) on page 1476
- Assignment resource (page description) on page 1477
- Attestation - Assignment resource (page description) on page 1479

Displaying attestors of assignment resource pending attestation cases

You can see identities that still have to approve assignment resource attestation cases.

To show attestors of an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the (pending) attestation case that has attestors you want to display.
8. In the details pane, click **Actions** > **Send a reminder mail**.

   The **Send a reminder mail** dialog lists all the identities that can approve this attestation case. You can now send these identities a reminder.

To show attestors of all attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **View approvers for pending cases**.

   The **Send a reminder mail** dialog shows all the identities that still have attestation cases to approve. You can now send these identities a reminder.

Related topics

- Attestors for attestation cases on page 163
- Governance administration (page description) on page 1363
- Assignment resources (page description) on page 1476
- Assignment resource (page description) on page 1477
- Attestation - Assignment resource (page description) on page 1479

Approving and denying assignment resource attestation cases

You can grant or deny approval to attestation cases of assignment resources.

To approve an attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to decide approval on.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Approve**.
8. On the **Attestation - <assignment resource>** page, perform one of the following actions:
   - Click (**Approve**) next to the attestation case you want to approve.
   - Click (**Deny**) next to the attestation case you want to deny.

   TIP: To grant or deny approval for all the attestation cases displayed, click (**Approve all**) or (**Deny all**).
9. Click **Next**.
10. (Optional) On the **Pending Attestations – Approvals** page, perform one of the following actions:
    - For approved attestation case:
      - To provide a reason for all approved attestation cases, enter the reason in the **Reason for approvals** field.
      - To use a predefined standard reason for all approved attestation cases, select the reason in the **Standard reason** list.
    - For denied attestation cases:
      - To provide a reason for all denied attestation cases, enter the reason in the **Reason for approvals** field.
      - To use a predefined standard reason for all denied attestation cases, select the reason in the **Standard reason** list.
    - To provide an individual reason for an approval decision, click **Enter a reason** and enter your reason.

    TIP: By giving reasons, your approvals are more transparent and support the audit trail.

NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

11. Click **Save**.

Related topics

- Attestation on page 153
- Governance administration (page description) on page 1363
- Assignment resources (page description) on page 1476
- Assignment resource (page description) on page 1477
- Attestation - Assignment resource (page description) on page 1479

Sending reminders about assignment resource pending attestation cases

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

The following options are available for sending reminders:

- You can select a specific attestation case that shows its attestors and then send a reminder about this attestation case to one specific attestor (see Option 1).
- You can send a reminder to all attestors of pending attestation cases that are shown on the current tab. This allows you to quickly notify all attestors that still need to make an approval decision (see Option 2).
- You can show all the attestors that still need to make approval decisions about attestation cases and then send a reminder to one specific attestor (see Option 3).

To send a reminder to attestors of a selected attestation case

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the list, click the attestation case that has attestors you want to remind.
8. In the details pane, click **Actions** > **Send a reminder mail**.
9. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
10. Select the email program that you want to use.

This opens an email template with the attestor's email address.

11. Edit the email and send it to the attestor.

To send a reminder to all the attestors of pending attestation cases on the current tab

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
7. Click **Send reminder**.
8. In the **Send a reminder mail** dialog, enter the message for the attestor.
9. Click **OK**.

To send a reminder a specific attestor about pending attestation cases

1. In the menu bar, click **Responsibilities** > **Governance Administration**.
2. On the **Governance Administration** page, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose attestation cases you want to display.
4. In the details pane, click **Edit**.
5. On the overview page, click **Attestation**.
6. (Optional) On the **Attestations – <assignment resource name>** page, click on a tab to display the corresponding attestation cases.
7. In the **Send a reminder mail** dialog, next to the identity you want to notify, click **Send a mail**.
8. Select the email program that you want to use.

   This opens an email template with the attestor's email address.
9. Edit the email and send it to the attestor.

Related topics

- Sending attestation reminders on page 167
- Sending attestation reminders on page 167
- Governance administration (page description) on page 1363
- Assignment resources (page description) on page 1476

- Assignment resource (page description) on page 1477
- Attestation - Assignment resource (page description) on page 1479

7

Applications

You may be able to access other applications, as configured by your system administrator. This provides you with a shortcut to other web applications deemed of value by your company.

NOTE: If you are a system administrator, and would like to add applications, see the One Identity Manager Web Designer Reference Guide.

To access other web applications from the Web Portal

- Open **Applications** and select the required web application.

  The application may appear within the Web Portal, or in a separate window, depending on how the system administrator configured it.

Calls

In the **Calls** menu, you can add new calls or view all calls in the call history.

Detailed information about this topic

- Adding new calls on page 793
- Call history on page 793

Adding new calls

When you add new calls, you report problem cases with different causes. For example, a call can be added for an employee who reports a problem or for products for which conditions of contact were specified. Even a device or workdesk associated with the problematic device, can play a part when adding a call.

To add a new call

1. Open **New Call**.
2. Enter a detailed description of the problem and select the affected product.
3. Set the severity of the problem in **Severity** and select a cost center using **Assign**.
4. Select an additional identity using **Assign** and click **Save**.

Call history

In the **Call History** view, you can see all placed calls.

NOTE: Use the check boxes at the top of the section to limit the calls shown.

To view a specific call

1. Open **Call history** and select a call from the list.

   In the details pane, there is more information about the call. You can subsequently change **Severity**, **Description** and **Product** entries on the **Main Data** tab.
2. View the staff involved, status, and measures taken on the **History** tab.
3. View attachments on the **Attachments** tab.
4. Click **Save**.

Removing attachments

In the **Call History** menu, you can remove single files that have been added as attachments to a call.

To remove a file from a call's attachments

1. Open **Call history** and select a call from the list.
2. In the details pane, select the **Attachments** tab and click next to the file.
3. Confirm the message with **Yes**.

   This removes the file from the **Attachments** tab.

Discovering your statistics on the home page

Statistics are graphical summaries of the information pertaining to you. You can open your statistics on the home page taking your permissions into account.

NOTE: In earlier versions of the Web Portal, these statistics are located under **Access Governance**.

More statistics about managed organizations, system entitlements, business roles and system roles are available for managers in **My Responsibilities**.

The data on the home page is updated daily. You can customize the data you see on the dashboard by selecting the objects you want to include, and which statistics you want to show for each object. Checking your dashboard regularly can help you understand any issues that need addressing. For more information, see What statistics are available? on page 800.

Detailed information about this topic

Statistics

Graphical representation of data is depicted by diagrams. Heatmaps also provide data in graphical form. For more information, see Heatmap on page 798.

Table 55: Icons used in diagrams

Icon	Meaning
⚠	The value in this statistic is in the balance. It is neither critical nor compliant. You should keep an eye on this value or statistic.

Icon	Meaning
	This value has not changed. The date of last change is shown.
	This icon verifies that the value in this statistic compliant. The arrow icon displayed in combination with this icon is also green and provides more detailed information about changes to the value.
	This icon indicates that the value in this statistic is in the critical range. The arrow icon displayed in combination with this icon also means critical and provides more detailed information about changes to the value.
	This arrow icon shows an increasing value since the last change and is colored green. The value is still in a compliant range. The difference since the last change is shown.
	This arrow icon shows a decreasing value since the last change and is colored green. The value is still in a compliant range. Moving the mouse over the icon shows the difference since the last change.
	This arrow icon shows an increasing value since the last change and is colored red. The value is in the non-compliant range and more critical than before. The difference since the last change is shown.
	This arrow icon shows a decreasing value since the last change and is colored red. The value is in the non-compliant range but better than before. Moving the mouse over the icon shows the difference since the last change.

Detailed information about this topic

- Viewing statistics on page 796
- Hiding statistics on page 797
- Viewing source data on page 797
- Apply filter on page 797

Viewing statistics

The use of HyperViews, heatmaps, and statistics differs between the desktop view and the mobile view. For more information, see Heatmaps and statistics in the mobile view on page 51.

To open a statistics view

1. Select the home page .

   Roles and organizations are displayed on the home page.
2. Click the role or organization you want to see in more detail.

Depending on your selection, you are shown statistics either in form of a table or a heatmap. There are also, however, roles, or organizations, which take you to a page with source data.

Hiding statistics

You can hide statistic, which are not relevant. These you can show again at any time over your **Personal Dashboard Settings** in the **Settings**. For more information, see Personal dashboard settings on page 59.

To hide statistics

1. Select the home page using .

   Roles and organizations are displayed on the home page.

2. Click the role or organization you want to see in more detail.
3. Click the selected role's view.
4. Disable one or more statistics in the list that you do not want to see anymore.
5. Close the dialog.

   This hides the selected statistics.

Viewing source data

You can only view source data for certain roles and organizations. You can view a heatmap or statistics, with graphical representation, through certain roles or organizations.

To view source data from a role or organization

1. Select the home page.

   Roles and organizations are displayed on the home page. These roles or organizations are divided into their associated subgroups.

2. Click the role or organization you want to view in more detail, for example, departments without managers.

   This displays a view with the corresponding data.

Apply filter

You can filter the information displayed on your dashboard to suit you own requirements.

To customize the information displayed on a statistics view

- Apply a filter to the statistic view.

  This opens a dialog for the selected filter. For more information, see Filtering on page 40.

  NOTE: The filter function is not available for all statistics.

Heatmap

The heatmap in the Web Portal presents roles and organizations as colored squares. They are intended to help you quickly visualize particularly prominent values within a large amount of data and to comprehend them at a glance. The size of the rectangles corresponds to the relative size of the role or organization. The more identities you have in a company's structure, for example, the larger the rectangle in the view.

NOTE: An overview of the company structures you manage is displayed on the home page.

The rectangle colors correspond to a selectable, linked-in data value, and range from red to green, where red stands for a value tending to require more attention. Red indicates, for example, a lot of compliance rule violations or identities with high risk indexes. Yellow indicates for an average, which can also mean that there has been no changes to this company structure since the last analysis. The heatmap not only provides a clear overview of the current data, but also provides another useful function by making a historical comparison to previous data.

You can see the following risky results or properties in a heatmap.

- Policy violations
- Average number of permissions per identity
- Highest identity risk index
- Average identity risk index
- Rule violations
- Highest resource risk index by host

NOTE: Hyper Views, heatmaps, and statistics have different behavior in the desktop view as opposed to the mobile view. For more information, see Heatmaps and statistics in the mobile view on page 51.

Detailed information about this topic

- Viewing data on page 799
- Viewing changes for a specific period on page 799
- Limiting the amount of data on page 799
- Displaying object details on page 799

Viewing data

Without having set any preferences, the color map is displayed as a data value when you open it, for example, for the number of compliance rules.

To view data from a role or organization

1. Select the home page.
2. If available, click the role or organization in the form of a heatmap that you would like to view more closely.

   NOTE: In the first field, you can set the size of the square. Available settings are **Dynamic size** and **Unisize**.
3. Limit your selection by selecting one or more objects with **Change**.
4. Confirm your selection by clicking **Close**.

   You selection is displayed to the left of **Change**.

Viewing changes for a specific period

In a heatmap you can view data within a specific time period.

To view data for a specific time period

- Select the required entry from the second field, for example "Month-to-date changes".

  The data is displayed in the heatmap according to your selection.

Limiting the amount of data

You can limit the amount of data displayed in the heatmap by using the slide rule.

To limit the size of the data

- Click one of the slide rules in the scale at the bottom of the view to limit the data size.

  NOTE: You may be shown up to 500 data sets graphically.

Displaying object details

To get more information, you can call up object details about an rectangle in a heatmap.

To obtain more information about individual roles or organizations

1. Click the rectangle in the view after you have configured your settings and the Web Portal has adjusted the view accordingly.

   Another shape is displayed for the rectangle with additional information.

   NOTE: To display additional information about the role or organization you are interested in, hover the mouse over the corresponding rectangle. This information is not so comprehensive and is there to provide initial orientation within the heatmap.

2. Perform one of the following tasks:

   a. Click one of the items to obtain more information.

   b. Select more information through **View object details**.

   A view with detailed information, spread over several tabs, is displayed for the square you click.

What statistics are available?

The statistics and heatmaps you see in the Web Portal depend on your roles and permissions. Only statistics relevant to you are available on the home page.

Statistics can be customized to display the objects and statistics that interest you. You can also sort and filter statistical information or export it as a report. For more information, see Discovering your statistics on the home page on page 795.

Detailed information about this topic

- Displaying high risk objects on page 800
- Compliance on page 801
- Risk on page 802
- Policies on page 803
- Organization on page 803
- IT Shop on page 804
- Attestations on page 805
- Target systems on page 805

Displaying high risk objects

You can display an overview of the objects with the highest risk factor in Web Portal. This can help you prioritize when managing your business resources. Company resources have risk values, which provide the risk index when combined with risk index functions.

To display the high risk object overview

1. In the menu bar, click **Compliance** > **Governance Administration**.
2. On the **Governance Administration** page, click **High Risk Overview**.

   This opens the **High Risk Overview** page (see High risk overview (page description) on page 1005).
3. (Optional) Click a section header to display the corresponding objects.
4. (Optional) To display all high risk objects, select the check box next to **Show all high risk objects**.

Related topics

- Governance administration (page description) on page 1001
- High risk overview (page description) on page 1005

Compliance

| NOTE: This function is only available if the module Compliance Rules Module is installed.

The Manager can be used to define rules for maintaining and monitoring regulatory requirements and automatically deal with rule violations. Rules are used for locating rule violations and to prevent them.

Statistics are available on the following topics.

Table 56: Overview of statistics on compliance rules

Statistics	Description
Pending rule violations	Show all types of rule violations.
Compliance violations	Shows compliance violations This statistic is available for different company structures. • Department • Location • Cost center • Business role
Compliance violations according to rules	Shows compliance rule violations for each rule.
New rule violations	Show new rule violations. This statistic is also available for new rule violations in recent months.

Statistics	Description
Overdue rule violations	Shows overdue rule violations.
Assignments that contribute to violations	Show assignments that contributed to violations.
Last approvals granted (rule violations)	Show the last granted approvals that contributed to rule violations.
Cost centers with increased violations	Show the cost centers that stand out due to a high rate of violations. This statistic is also available for other company structures. • Departments • Locations
Last approvals (rule violations)	Show the last approvals that contributed to rule violations.

For more information, see Compliance – Governance Administration on page 209.

Risk

There are various statistics available to you for risk assessment. The following statistics are available for this topic.

Table 57: Risk assessment statistics

Statistics	Description
Number of active employees with a risk index of more than 0.5	Displays the number of active identities with a risk index more than the critical value.
Highest person risk index by department	Displays the highest risk index of all identities by department. This statistic is also available for other company structures. • Location • Cost center • Business role
Average person risk index by department	Displays the average risk index of identities by department. This statistic is also available for other company structures. • Location

Statistics	Description
	• Cost center • Business role
Employees by risk index	Displays all identities that can be assigned to the same risk index.

Policies

Other, different statistics are available for company policies.

Table 58: Company policy statistics

Statistics	Description
Pending Policy Violations	Shows pending policy violations.
Overdue policy violations	Shows overdue policy violations.
Policy violations by department	Shows policy violations by department. This statistic is available for different company structures. • Location • Cost center • Business role
New policy violations	Shows new policy violations. This statistic is also available for new policy violations within the last month.
Policy violations (actual)	Shows current policy violations. This statistic is also available for new policy violations within the last seven days.
Policy violation approval rates	Shows the approval rate for policy violations.
Last approvals (policy violations)	Show the last approvals, which contributed to policy violations.
Last approvals granted (policy violations)	Show the last granted approvals, which contributed to policy violations.

Organization

The following statistics are displayed for departments that you manage.

- Information about identity accounts
- Information about identities
- Rule violations
- Information about pending requests
- The top roles and entitlements

For more information, see Managing my departments on page 220.

IT Shop

The IT Shop is the tool that identities use to make requests. These statistics help you to answer the following questions.

- Which products are the most popular, both by product owner and by shop
- How fast requests are processed
- Request frequency over time

Table 59: Statistics about IT shop structures

Statistics	Description
Pending requests	Displays all pending requests.
Open requests by service category	Displays all pending requests by service category. This statistic contains other criteria. • By next approver • By recipient
Last approvals granted (Shop)	Shows the last approvals granted for requests.
New requests	Shows new requests.
Number of requestable products	Shows the number of products that can be requested.
Denied requests by service category	Shows denied requests by service category.
Average request processing time by shop	Show the average processing time of a request by shop.
Top 10 requested products by shop	Shows the top 10 requested products by shop. This statistic is also available for the top 10 requested products by product owner.
Request frequency (12 months)	Shows the frequency of requests within the last 12 months.

Statistics	Description
	This statistic is also available for the frequency of requests within the last 12 months by owner.

For more information, see Managing my departments on page 220.

Attestations

There are a number of statistics available to you for attestation cases. The following statistics are available.

Table 60: Attestation case statistics

Statistics	Description
Pending attestation cases	Displays all open attestation cases. This statistic contains other criteria. • By policy • By next approver • By framework
Attestation approval rates	Shows the approval rate for attestation.
Decided attestation approvals within/over the limit	Shows attestation approvals decisions within/over the limit. This statistic is also available for pending attestation cases within/over the limit.
Attestation status by type	Show attestation status by type.
Attestations	Shows all attestations.
Last approvals (attestation)	Shows the most recent attestation approval decisions. This statistic is also available for attestations that have been granted approval.
Overdue attestations	Displays overdue attestations.

Target systems

There are a number of statistics available to you for target systems. The following statistics are available.

Table 61: Target system statistics

Statistics	Description
Pending attestation by system entitle-ments	Displays pending attestation by system entitle-ments.
Number of user accounts with a risk index of more than {0}	Displays the number of user accounts with a risk index more than specified value. This statistic is also available for the number of entitlements with a risk index more than specified value.
User accounts having risk higher {0} by domain	Displays user accounts with a risk index more than specified value by domain. This statistic contains other criteria. • Entitlements having risk higher that a specified value by domain. • Entitlements having risk higher that a specified value by department.
Employees without user accounts	Displays identities without user accounts.
Entitlements without requests	Displays entitlements without a request. This statistic contains other criteria. • Active Directory • Oracle E-Business Suite • LDAP • SAP R/3 • SharePoint
Groups with / without user account assignments	Displays groups with or without user account assignments. This statistic contains other criteria. • Active Directory • LDAP • SAP R/3 • SharePoint • Notes • Groups, roles, and profiles with/without user account assignments SAP R/3
Inactive identities with enabled user	Displays inactive identities that have an enabled

Statistics	Description
accounts	user account.
Locked user accounts of enabled employees	Displays locked user accounts of active identities.

Appendix: Attestation conditions and approval policies from attestation procedures

When attestation policies are created or edited (see Setting up attestation policies on page 156 or Editing attestation policies on page 157), you specify attestation conditions and approval policies:

- Attestation procedures specify which objects to attest. They define the properties of the attestation objects to attest.
- There are different attestation conditions for each attestation procedure that you use to specify which objects to attest.
- Attestors for each attestation case are determined by approval policies.

In the following chapter, you will find more information about the various attestation procedures and associated approval policies and attestation conditions.

Attesting primary departments

Primary identity memberships in departments are attested using the **Primary department attestation** attestation procedure.

Condition	Description
All departments	Attests primary memberships in all departments.
Specific departments	Select the departments with primary memberships to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific child departments	Select the departments with primary memberships to attest. In addition, primary memberships of all child departments under this department are attested.

Condition	Description
	Use and to switch between hierarchical and list view. Multi-select is possible.
Departments with defined risk index	Use the ruler to specify a risk index range. Attests primary memberships in departments with a risk index in the chosen range.
Departments with matching name	Enter part of a name of departments with primary memberships to attest. All departments that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting primary business roles

Primary identity memberships in business roles are attested using the **Primary business role attestation** attestation procedure.

Condition	Description
All business roles	Attests primary memberships in all business roles.
Specific business roles	Select the business roles with primary memberships to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific child business roles	Select the business roles with primary memberships to attest. In addition, primary memberships of all child business roles under this business role are attested. Use and to switch between hierarchical and list view. Multi-select is possible.
Business roles with specific role classes	Select the role classes. Attests primary membership in business roles with this role class.
Business roles with defined risk index	Use the ruler to specify a risk index range. Attests primary memberships in business roles with a risk index in the chosen range.
Business roles with matching name	Enter part of a name of business roles with primary memberships to attest. All business roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting primary cost centers

Primary identity memberships in cost centers are attested using the **Primary cost center attestation** attestation procedure.

Condition	Description
All cost centers	Attests primary memberships in all cost centers.
Specific cost centers	Select the cost centers with primary memberships to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific child cost centers	Select the cost centers with primary memberships to attest. In addition, primary memberships of all child cost centers under this cost center are attested. Use and to switch between hierarchical and list view. Multi-select is possible.
Cost centers with defined risk index	Use the ruler to specify a risk index range. Attests primary memberships in cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with primary memberships to attest. All cost centers that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting primary locations

Primary identity memberships in locations are attested using the **Primary location attestation** attestation procedure.

Condition	Description
All locations	Attests primary memberships in all locations.
Specific locations	Select the locations with primary memberships to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific child locations	Select the locations with primary memberships to attest. In addition, primary memberships of all child locations under this location are attested. Use and to switch between hierarchical and list view. Multi-select is

Condition	Description
	possible.
Locations with defined risk index	Use the ruler to specify a risk index range. Attests primary memberships in locations with a risk index in the chosen range.
Locations with matching name	Enter part of a name of locations with primary memberships to attest. All locations that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting secondary departments

Secondary identity memberships in departments are attested using the **Secondary department attestation** attestation procedure.

Condition	Description
All departments	Attests secondary memberships in all departments.
Specific departments	Select the departments with secondary memberships to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific child departments	Select the departments with secondary memberships to attest. In addition, secondary memberships of all child departments under this department are attested. Use and to switch between hierarchical and list view. Multi-select is possible.
Departments with defined risk index	Use the ruler to specify a risk index range. Attests secondary memberships in departments with a risk index in the chosen range.
Departments with matching name	Enter part of a name of departments with secondary memberships to attest. All departments that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting secondary cost centers

Secondary identity memberships in cost centers are attested using the **Secondary cost center attestation** attestation procedure.

Condition	Description
All cost centers	Attests secondary memberships in all cost centers.
Specific cost centers	Select the cost centers with secondary memberships to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific child cost centers	Select the cost centers with secondary memberships to attest. In addition, secondary memberships of all child cost centers under this cost center are attested. Use and to switch between hierarchical and list view. Multi-select is possible.
Cost centers with defined risk index	Use the ruler to specify a risk index range. Attests secondary memberships in cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with secondary memberships to attest. All cost centers that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting secondary locations

Secondary identity memberships in locations are attested using the **Secondary location attestation** attestation procedure.

Condition	Description
All locations	Attests secondary memberships in all locations.
Specific locations	Select the locations with secondary memberships to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific child locations	Select the locations with secondary memberships to attest. In addition, secondary memberships of all child locations under this location are attested. Use and to switch between hierarchical and list view. Multi-select is

Condition	Description
	possible.
Locations with defined risk index	Use the ruler to specify a risk index range. Attests secondary memberships in locations with a risk index in the chosen range.
Locations with matching name	Enter part of a name of locations with secondary memberships to attest. All locations that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting PAM asset groups

PAM asset groups are attested using the **PAM asset group attestation** attestation procedure.

Condition	Description
All PAM asset groups	Attests all PAM assets groups.
Specific PAM asset groups	Select the PAM asset groups to attest.
PAM asset groups on specific systems	Select the PAM appliances with PAM asset groups to attest.
PAM asset groups with matching name	Enter part of a name of PAM asset groups with access to attest. All PAM asset groups that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting PAM asset accounts

PAM asset accounts are attested using the **PAM asset account attestation** attestation procedure.

Condition	Description
All PAM asset accounts	Attests all PAM asset accounts.

Condition	Description
Specific PAN asset accounts	Select the PAM asset accounts to attest.
PAM asset accounts on specific systems	Select the PAM appliances with PAM asset accounts to attest.
PAM asset accounts with matching name	Enter part of a name of PAM asset accounts with access to attest. All PAM asset accounts that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting PAM assets

PAM assets are attested using the **PAM asset attestation** attestation procedure.

Condition	Description
All PAM assets	Attests all PAM assets.
Specific PAM assets	Select the PAM assets to attest.
PAM assets on specific systems	Select the PAM appliances with PAM asset to attest.
PAM assets with matching name	Enter part of a name of PAM assets with access to attest. All PAM assets that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting PAM user groups

PAM user groups are attested using the **PAM user group attestation** attestation procedure.

Condition	Description
All PAM user groups	Attests all PAM user groups.

Condition	Description
Specific PAM user groups	Select the PAM user groups to attest.
PAM user groups with matching name	Enter part of a name of PAM user groups with access to attest. All PAM user groups that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting PAM user accounts

PAM user accounts are attested using the **PAM user account attestation** attestation procedure.

Condition	Description
All PAM user accounts	Attests all PAM user accounts.
Specific permissions	Select the permissions. Attests PAM user accounts with these permissions.
Specific PAM user accounts	Select the PAM user accounts to attest.
PAM user accounts in specific user groups	Select the user groups. Attests PAM user accounts that belong to these user groups.
PAM user groups on specific systems	Select the PAM appliances with PAM user groups to attest.
PAM user accounts mapped to specific employees	Select the identities. Attests PAM user accounts that are assigned these identities.
PAM user accounts with matching name	Enter part of a name of PAM user accounts with access to attest. All PAM user accounts that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting PAM account groups

PAM account groups are attested using the **PAM account group attestation** attestation procedure.

Condition	Description
All PAM account groups	Attests all PAM account groups.
Specific PAM account groups	Select the PAM account groups to attest.
PAM user accounts on specific systems PAM account groups on specific systems	Select the PAM appliances with PAM user accounts to attest. Select the PAM appliances with PAM account groups to attest.
PAM account groups with matching name	Enter part of a name of PAM account groups with access to attest. All PAM account groups that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting PAM directory accounts

PAM directory accounts are attested using the **PAM directory account attestation** attestation procedure.

Condition	Description
All PAM directory accounts	Attests all PAM directory accounts.
Specific PAM directory accounts	Select the PAM directory accounts to attest.
PAM directory	Select the directories. Attests directory accounts that are found in this

Condition	Description
accounts on specific directories	directory.
PAM directory accounts with matching name	Enter part of a name of PAM directory accounts with access to attest. All PAM directory accounts that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting PAM accesses

PAM access are attested using the **PAM access attestation** attestation procedure.

Condition	Description
All PAM accesses	Attests all PAM access.
Specific PAN asset accounts	Select the PAM asset accounts with access to attest.
Specific PAM assets	Select the PAM assets with access to attest.
Specific PAM user accounts	Select the PAM user accounts with access to attest.
Specific PAM directory accounts	Select the PAM directory accounts with access to attest.
Specific PAM directories	Select PAM directories. Attests access to these PAM directories.
Specific access type	Select access types. Attests access that uses one of these access types.
PAM user accounts mapped to specific employees	Select the identities. Attests access through PAM user accounts with these identities assigned to them.
PAM user accounts with defined risk index	Use the ruler to specify a risk index range. Attests access through PAM user accounts with a risk index in the chosen range.

Condition	Description
PAM user accounts with matching name	Enter part of a name of PAM user accounts with access to attest. All PAM user accounts that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting departments

Department properties are attested using the **Department attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All departments	Attests all departments.
Specific departments	Select the departments to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Departments with defined risk index	Use the ruler to specify a risk index range. Attests departments with a risk index in the chosen range.
Departments with matching name	Enter part of a name of departments with access to attest. All departments that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases.
Attestation of departments by manager	Department managers can make approval decisions through attestation cases.

Application role attestation

Application role properties are attested using the **Application role attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All application roles	Attests all application roles.
Specific application roles	Select the application roles to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Application roles with defined risk index	Use the ruler to specify a risk index range. Attests application roles with a risk index in the chosen range.
Application roles with matching name	Enter part of a name of application roles with access to attest. All application roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases.

Business role attestation

Business role properties are attested using the **Business role attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All business roles	Attests all business roles.
Specific business roles	Select the business roles to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Business roles with specific role classes	Select the role classes. Attests business roles with these role classes.
Business roles with defined risk index	Use the ruler to specify a risk index range. Attests business roles with a risk index in the chosen range.
Business roles with matching name	Enter part of a name of business roles with access to attest. All business roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click **Assign**/**Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases.
Attestation of business roles by manager	Business role managers can make approval decisions through attestation cases.
Certification of business roles	Business role managers can make approval decisions through attestation cases.

Attesting system roles

Cost center properties are attested using the **Cost center attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All cost centers	Attests all cost centers.
Specific cost centers	Select the cost centers to attest. Use and to switch between hierarchical and list view. Multi-

Condition	Description
	select is possible.
Cost centers with defined risk index	Use the ruler to specify a risk index range. Attests cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with access to attest. All cost centers that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases.
Attestation of cost centers by manager	Cost center managers can make approval decisions through attestation cases.

Attesting locations

Location properties are attested using the **Location attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All locations	Attests all locations.
Specific locations	Select the locations to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Locations with defined risk index	Use the ruler to specify a risk index range. Attests locations with a risk index in the chosen range.
Locations with matching name	Enter part of a name of locations with access to attest. All locations that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases.
Attestation of locations by manager	Location managers can make approval decisions through attestation cases.

Attesting system roles

System role properties are attested using the **System role attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All system roles	Attests all system roles.
Specific system roles	Select the system roles to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
System roles by applications	Select the applications (Application Governance). Attests system roles that are assigned to these applications.
System roles with defined risk index	Use the ruler to specify a risk index range. Attests system roles with a risk index in the chosen range.
System roles with matching name	Enter part of a name of system roles with access to attest. All system roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases.
Attestation of system roles by manager	System role managers can make approval decisions through attestation cases.

Attesting memberships in system entitlements

User account memberships in system entitlements are attested using the **System entitlements membership attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All system entitlements	Attests memberships in all system entitlements.
Specific employees	Select the identities. Attests this identity's memberships (or their associated user accounts) in system entitlements.
Specific employees with subidentities.	Select the identities. Attests this identity's memberships (or their associated user accounts) in system entitlements. In addition, it attests sub identities' memberships (or their associated user accounts) that the select identities are assigned to.
Specific system entitlements	Select the system entitlements. Attests memberships in these system entitlements.
Membership by attestation state	Select an attestation status Attests memberships in system entitlements that match this attestation status. • **Denied memberships**: Attests memberships that have been denied. • **All Memberships**: Attests all memberships. • **New memberships**: Attests memberships that have never been attested.
New or not attested for x days	Specify a number of days. Attests memberships in system entitlements that have not been attested for the defined number of days.
No dynamic groups from Active Roles	Attests memberships in all system entitlements. Dynamic groups are ignored in the process.
System entitle-ments with specific owners	Select the identities. Attests memberships in system entitlements that are managed by these identities.
System entitle-ments in a target system container	Select the target system containers. Attests memberships in system entitlements found in these target system containers.

Condition	Description
System entitlements in target systems	Select the target systems. Attests memberships in system entitlements assigned to these target systems.
System entitlements with defined risk index	Use the ruler to specify a risk index range. Attests memberships in system entitlements with a risk index in the chosen range.
System entitlements with owners in departments	Select the departments. Attests memberships in system entitlements that are managed by the identities in these departments.
System entitlements with any owner	Attests user account memberships in system entitlements that only have one owner.
System entitlements with matching name	Enter part of a name of system entitlements with user account memberships to attest. All system entitlements that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
System entitlements by applications	Select the applications. Attests user account memberships in system entitlements that are assigned to these applications.
System entitlements by assignment origin	Select how user account memberships in system entitlements must be assigned to enable attestation: • **Directly assigned**: Attests memberships that were assigned directly. • **By request**: Attests memberships in system entitlements that were requested. • **By dynamic roles**: Attests memberships in system entitlements that were assigned through dynamic roles. • **Through roles**: Attests memberships in system entitlements that were assigned through roles. • **Through system roles**: Attests memberships in system entitlements that were assigned through system roles.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attest-

Approval policies	Description
	ation cases.
Attestation by selected approvers with automatic removal of assignments	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.
Attestation by entitlement owner with automatic removal of assignments	Product owners of system entitlements can be approved through attestation cases. Memberships are deleted if attestation is denied and the configuration fits.
Attestation by employee manager and product owner (with peer group analysis)	The following identities can be approved through attestation cases: • Identity managers who are assigned the system entitlements • Product owners of system entitlements after a peer group analysis (see Attestation by peer group analysis on page 162)
Attestation of group memberships by product owner with automatic removal of memberships	Product owners of system entitlements can be approved through attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

Attesting memberships in application roles

Memberships in application roles are attested using the **Application role membership attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All roles	Attests memberships in all applications roles.
Application roles with matching name	Enter part of a name of application roles with primary memberships to attest. All application roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
Attesting by attestation status	Select an attestation status Attests memberships in application roles that match this attestation status. You can select the follow status:

Condition	Description
	• **Denied memberships**: Attests memberships that have been denied. • **All Memberships**: Attests all memberships. • **New memberships**: Attests memberships that have never been attested.
Specific employees	Select the identities. Attests identity memberships in application roles.
Specific employees with subidentities.	Select the identities. Attests identity memberships in application roles. In addition, this identity's subidentities memberships in application roles are attested.
Specific roles	Select the application roles. Attests memberships in these application roles. Use and to switch between hierarchical and list view. Multi-select is possible.
New or not attested for x days	Specify a number of days. Attests memberships in application roles that have not been attested for the defined number of days.
Roles by assign-ment type	Select how memberships in application roles must be assigned to enable attestation: • **Directly assigned**: Attests memberships that were assigned directly. • **By request**: Attests memberships that were requested. • **By delegation**: Attests memberships that were delegated.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers with automatic removal of assignments	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

Attestation of memberships in business roles

Memberships in business roles are attested using the **Business role membership attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All roles	Attests memberships in all business roles.
Business roles with matching name	Enter part of a name of business roles with memberships to attest. All business roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
Attesting by attestation status	Select an attestation status Attests memberships in business roles that match this attestation status. You can select the follow status: • **Denied memberships**: Attests memberships that have been denied. • **All Memberships**: Attests all memberships. • **New memberships**: Attests memberships that have never been attested.
Specific employees	Select the identities. Attests identity memberships in business roles.
Specific employees with subidentities.	Select the identities. Attests identity memberships in business roles. In addition, this identity's subidentities memberships in business roles are attested.
Specific roles	Select the business roles. Attests memberships in these business roles. Use and to switch between hierarchical and list view. Multi-select is possible.
New or not attested for x days	Specify a number of days. Attests memberships in business roles that have not been attested for the defined number of days.
Roles with specific owners	Select the identities. Attests memberships in business roles of identities who are owners of these business roles.
Roles with specific role classes	Select the role classes. Attests membership in business roles of this role class.

Condition	Description
Roles with defined risk index	Use the ruler to specify a risk index range. Attests memberships in business roles with a risk index in the chosen range.
Roles with any owner	Attests all memberships in business roles that have an owner.
Roles with owners in departments	Select the departments. Attests all business roles that have an owner in the selected department.
Roles by assignment type	Select how memberships in business roles must be assigned to enable attestation: • **Directly assigned**: Attests memberships that were assigned directly. • **By request**: Attests memberships that were requested. • **By delegation**: Attests memberships that were delegated. • **By dynamic role**: Attests memberships that were attested through dynamic roles.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers with automatic removal of assignments	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

Attesting assignment of memberships in system roles

Memberships in system roles are attested using the **System role membership attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All roles	Attests memberships in all system roles.
System roles with matching name	Enter part of a name of system roles with memberships to attest. All system roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
Attesting by attestation status	Select an attestation status Attests memberships in system roles that match this attestation status. You can select the follow status: • **Denied memberships**: Attests memberships that have been denied. • **All Memberships**: Attests all memberships. • **New memberships**: Attests memberships that have never been attested.
Specific roles	Select the system roles. Attests memberships in these system roles. Use and to switch between hierarchical and list view. Multi-select is possible.
New or not attested for x days	Specify a number of days. Attests memberships in system roles that have not been attested for the defined number of days.
Roles with specific owners	Select the identities. Attests memberships in system roles of identities who are owners of these system roles.
Roles with defined risk index	Use the ruler to specify a risk index range. Attests memberships in system roles with a risk index in the chosen range.
Roles with any owner	Attests all memberships in system roles that have an owner.
Roles with owners in departments	Select the departments. Attests all system roles that have an owner in the selected department.
System roles by applications	Select the applications (Application Governance). Attests memberships in system roles assigned to these applications.
Roles by assignment type	Select how memberships in system roles must be assigned to enable attestation: • **Directly assigned**: Attests memberships that were assigned directly. • **By request**: Attests memberships that were requested. • **Inherited**: Attests inherited memberships.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers with automatic removal of assignments	Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

Attesting device owners

Owners of devices are attested by using the **Device ownership attestation** attestation procedure.

Condition	Description
All devices	Attests owners of all the devices.

Attesting system entitlement owners

Owners of system entitlements are attested by using the **System entitlement ownership attestation** attestation procedure.

Condition	Description
All system entitle-ments	Attests owners of all system entitlements.
System entitlements by applications	Select the applications. Attests system entitlements owners to which the applications are assigned.

Attesting system entitlement owners (initial)

Initial assignments of product owners to system entitlements are attested using the **System entitlement ownership attestation (initial)** attestation procedure (this means that the system entitlements did not have an product owner beforehand).

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All system entitle-ments without owner	Attests initial assignments of owners to system entitlements that do not have product owners.
No dynamic groups from Active Roles	Attests initial assignment of product owners to system entitlements. Dynamic groups are ignored in the process.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation of ownership by proposed new owner	The proposed new product owners can make approval decisions about attestation cases.

Attesting user accounts

User accounts are attested using the **User account attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All user accounts	Attests all user accounts.
All privileged user accounts	Attests all privileged user accounts.
User accounts in the target system	Select the target systems. Attests user accounts assigned to these target systems.
User accounts of specific employees	Select the identities. Attests user accounts assigned to these identities.
Specific user accounts	Select the user accounts to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
User accounts with defined risk index	Use the ruler to specify a risk index range. Attests user accounts with a risk index in the chosen range.
User accounts with matching name	Enter part of a name of user accounts with access to attest. All user accounts that have this pattern in their name are included.

Condition	Description
	Example: **Per** finds "Person", "Personal", "Perfection" and so on.
User accounts with employees in departments	Select the departments. Attests user accounts with identities assigned to these departments. Use and to switch between hierarchical and list view. Multi-select is possible.
User accounts of employees in child departments	Select the departments. Attests user accounts with identities assigned to these or their child departments. Use and to switch between hierarchical and list view. Multi-select is possible.
User accounts of employees with matching names	Enter part of a name of the identities with user accounts to attest. All identities that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests user accounts that have not been attested for the defined number of days.
All user accounts not assigned to an identity	Only attests user accounts not assigned to an identity (so-called orphaned user accounts).
Linked user accounts	Attests only user accounts that are assigned these identities.
Target system type	Select the target systems types. Attests user accounts in target system of this target system type.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click **Assign**/**Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases.
Attestation by target system manager	Target system managers can be approved through attestation cases.

Attesting system entitlements

System entitlements are attested using the **System entitlement attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All system entitlements	Attests all system entitlements.
Specific system entitlements	Select the system entitlements to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
No dynamic groups from Active Roles	Attests all system entitlements. Dynamic groups are ignored in the process.
System entitlements with defined risk index	Use the ruler to specify a risk index range. Attests system entitlements with a risk index in the chosen range.
System entitlements with matching name	Enter part of a name of system entitlements with access to attest. All system entitlements that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
System entitle-ments by applic-ations	Select the applications. Attests system entitlements that are assigned to these applications.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation of system entitlements by product owner (OA)	Product owners of system entitlements can be approved through attestation cases.
Attestation by target system manager	Target system managers can be approved through attestation cases.

Attesting assignment of system entitlement to departments

System entitlements assignments to departments are attested using the **Attestation of system entitlement assignments to departments** attestation procedure.

Condition	Description
All departments	Attests assignments of system entitlements to all departments.
All system entitle-ments	Attests assignments of all system entitlements to departments.
Attesting by attestation status	Select an attestation status Attests assignments of system entitlements, matching this attestation status, to departments. You can select the follow status: • **Denied memberships**: Attests assignments that have been denied. • **All Memberships:** Attests all assignments. • **New memberships**: Attests assignments that have never been attested.
Specific departments	Select the departments with system entitlements to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific system entitlements	Select the with system entitlements with assignments to departments to attest.
Departments with defined risk index	Use the ruler to specify a risk index range. Attests system entitlement assignments to departments with a risk index in the chosen range.
Departments with matching name	Enter part of a name of departments with system entitlement assignments to attest. All departments that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system entitlement assignments to departments that have not been attested for the defined number of days.
System entitle-ments with defined risk index	Use the ruler to specify a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to departments.
System entitle-ments with matching name	Enter part of a name of system entitlements with assignments to departments to attest. All system entitlements that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting assignment of system entitlement to business roles

System entitlements assignments to business roles are attested using the **Attestation of system entitlement assignments to business roles** attestation procedure.

Condition	Description
All business roles	Attests assignments of system entitlements to all business roles.
All system entitlements	Attests assignments of all system entitlements to business roles.
Attesting by attestation status	Select an attestation status Attests assignments of system entitlements, matching this attestation status, to business roles. You can select the follow status: • **Denied memberships**: Attests assignments that have been denied. • **All Memberships:** Attests all assignments. • **New memberships**: Attests assignments that have never been attested.
Specific business roles	Select the business roles with system entitlements to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific system entitlements	Select the with system entitlements with assignments to business roles to attest.
Business roles with specific role classes	Select the role classes. Attests system entitlement assignments to business roles with these role classes.
Business roles with defined risk index	Use the ruler to specify a risk index range. Attests system entitlement assignments to business roles with a risk index in the chosen range.
Business roles with matching name	Enter part of a name of business roles with system entitlement assignments to attest. All business roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system entitlement assignments to business roles that have not been attested for the defined number of days.
System entitle-	Use the ruler to specify a risk index range. Attests assignments of

Condition	Description
ments with defined risk index	system entitlements, with a risk index in the chosen range, to business roles.
System entitle-ments with matching name	Enter part of a name of system entitlement with assignments to business roles to attest. All system entitlements that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attestation of system entitlement assignments to cost centers

System entitlements assignments to cost centers are attested using the **Attestation of system entitlement assignments to cost centers** attestation procedure.

Condition	Description
All cost centers	Attests assignments of system entitlements to all cost centers.
All system entitle-ments	Attests assignments of all system entitlements to cost centers.
Attesting by attestation status	Select an attestation status Attests assignments of system entitlements, matching this attestation status, to cost centers. You can select the follow status: • **Denied memberships**: Attests assignments that have been denied. • **All Memberships:** Attests all assignments. • **New memberships**: Attests assignments that have never been attested.
Specific cost centers	Select the cost centers with system entitlements to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific system entitlements	Select the with system entitlements with assignments to cost centers to attest.
Cost centers with defined risk index	Use the ruler to specify a risk index range. Attests system entitlement assignments to cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with system entitlement assignments to attest. All cost centers that have this pattern in their

Condition	Description
	name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system entitlement assignments to cost centers that have not been attested for the defined number of days.
System entitlements with defined risk index	Use the ruler to specify a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to cost centers.
System entitlements with matching name	Enter part of a name of system entitlement with assignments to cost centers to attest. All system entitlements that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attestation of system entitlement assignments to locations

System entitlements assignments to locations are attested using the **Attestation of system entitlement assignments to locations** attestation procedure.

Condition	Description
All locations	Attests assignments of system entitlements to all locations.
All system entitlements	Attests assignments of all system entitlements to locations.
Attesting by attestation status	Select an attestation status Attests assignments of system entitlements, matching this attestation status, to locations. You can select the follow status: • **Denied memberships**: Attests assignments that have been denied. • **All Memberships:** Attests all assignments. • **New memberships**: Attests assignments that have never been attested.
Specific locations	Select the locations with system entitlements to attest. Use and to switch between hierarchical and list view. Multi-select is possible.

Condition	Description
Specific system entitlements	Select the with system entitlements with assignments to locations to attest.
Locations with defined risk index	Use the ruler to specify a risk index range. Attests system entitlement assignments to locations with a risk index in the chosen range.
Locations with matching name	Enter part of a name of locations with system entitlement assignments to attest. All locations that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system entitlement assignments to locations that have not been attested for the defined number of days.
System entitle-ments with defined risk index	Use the ruler to specify a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to locations.
System entitle-ments with matching name	Enter part of a name of system entitlement with assignments to locations to attest. All system entitlements that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting assignment of system role assignment to departments

System role assignments to departments are attested with the "Attestation of system role assignments to departments" attestation procedure.

Condition	Description
All departments	Assignments of system roles to all departments
All system roles	Attests assignments of all system roles to departments.
Attesting by attestation status	Select an attestation status Attests assignments of system roles, matching this attestation status, to departments. You can select the follow status: • **Denied memberships**: Attests assignments that have been denied. • **All Memberships:** Attests all assignments.

Condition	Description
	• **New memberships**: Attests assignments that have never been attested.
Specific departments	Select the departments with system roles to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific system roles	Select the with system roles with assignments to departments to attest.
Departments with defined risk index	Use the ruler to specify a risk index range. Attests system role assignments to departments with a risk index in the chosen range.
Departments with matching name	Enter part of a name of departments with system role assignments to attest. All departments that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system role assignments to departments that have not been attested for the defined number of days.
System roles with defined risk index	Use the ruler to specify a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to departments.
System roles with matching name	Enter part of a name of system role with departments assignments to attest. All system roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting assignment of system roles to business roles

System role assignments to business roles are attested with the "Attestation of system role assignments to business roles" attestation procedure.

Condition	Description
All business roles	Attests assignments of system roles to all business roles.
All system roles	Attests assignments of all system roles to business roles.
Attesting by	Select an attestation status Attests assignments of system roles,

Condition	Description
attestation status	matching this attestation status, to business roles. You can select the follow status: • **Denied memberships**: Attests assignments that have been denied. • **All Memberships:** Attests all assignments. • **New memberships**: Attests assignments that have never been attested.
Specific business roles	Select the business roles with system roles to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific system roles	Select the with system roles with assignments to business roles to attest.
Business roles with specific role classes	Select the role classes. Attests system roles assignments to business roles with these role classes.
Business roles with defined risk index	Use the ruler to specify a risk index range. Attests system role assignments to business roles with a risk index in the chosen range.
Business roles with matching name	Enter part of a name of business roles with system role assignments to attest. All business roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system role assignments to business roles that have not been attested for the defined number of days.
System roles with defined risk index	Use the ruler to specify a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to business roles.
System roles with matching name	Enter part of a name of system role with business roles assignments to attest. All system roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Cost center system role assignment attestation

System role assignments to cost centers are attested with the "Attestation of system role assignments to cost centers" attestation procedure.

Condition	Description
All cost centers	Attests assignments of system roles to all cost centers.
All system roles	Attests assignments of all system roles to cost centers.
Attesting by attestation status	Select an attestation status Attests assignments of system roles, matching this attestation status, to cost centers. You can select the follow status: • **Denied memberships**: Attests assignments that have been denied. • **All Memberships:** Attests all assignments. • **New memberships**: Attests assignments that have never been attested.
Specific cost centers	Select the cost centers with system roles to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific system roles	Select the with system roles with assignments to cost centers to attest.
Cost centers with defined risk index	Use the ruler to specify a risk index range. Attests system role assignments to cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with system role assignments to attest. All cost centers that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system role assignments to cost centers that have not been attested for the defined number of days.
System roles with defined risk index	Use the ruler to specify a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to cost centers.
System roles with matching	Enter part of a name of system role with cost center assignments to attest. All system roles that have this pattern in their name are

Condition	Description
name	included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting assignment of system entitlements to locations

System role assignments to locations are attested with the "Attestation of system role assignments to locations" attestation procedure.

Condition	Description
All locations	Attests assignments of system roles to all locations.
All system roles	Attests assignments of all system roles to locations.
Attesting by attestation status	Select an attestation status Attests assignments of system roles, matching this attestation status, to locations. You can select the follow status: • **Denied memberships**: Attests assignments that have been denied. • **All Memberships:** Attests all assignments. • **New memberships**: Attests assignments that have never been attested.
Specific locations	Select the locations with system roles to attest. Use and to switch between hierarchical and list view. Multi-select is possible.
Specific system roles	Select the with system roles with assignments to locations to attest.
Locations with defined risk index	Use the ruler to specify a risk index range. Attests system role assignments to locations with a risk index in the chosen range.
Locations with matching name	Enter part of a name of locations with system role assignments to attest. All locations that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system role assignments to locations that have not been attested for the defined number of days.
System roles	Use the ruler to specify a risk index range. Attests assignments of

Condition	Description
with defined risk index	system roles, with a risk index in the chosen range, to locations.
System roles with matching name	Enter part of a name of system role with location assignments to attest. All system roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Attesting assignments to system roles

Assignments to system roles are attested using the **System role membership attestation** attestation procedure.

Condition	Description
All system roles	Attests assignments to all system roles.
Attesting by attestation status	Select an attestation status Attests assignments to system roles, matching this attestation status. You can select the follow status: • **Denied memberships**: Attests assignments that have been denied. • **All Memberships:** Attests all assignments. • **New memberships**: Attests assignments that have never been attested.
Specific system roles	Select the with system roles with assignments to attest.
New or not attested for x days	Specify a number of days. Attests assignments to system roles that have not been attested for the defined number of days.
System roles by applications	Select the applications. Attests assignments to system roles assigned to these applications.
System roles with defined risk index	Use the ruler to specify a risk index range. Attests assignments to system roles with a risk index in the chosen range.
System roles with matching name	Enter part of a name of system role with assignments to attest. All system roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

Appendix: Page and menu descriptions

In this chapter you will find descriptions of pages and menus available in the Web Portal. The structure of the chapters follows the structure in the Web Portal.

Information (Menu description)

Use the various menu items in the 🔔 menu (**Information**) to perform the following actions:

- Display pending requests
- Display request inquiries
- Display pending attestations
- Display attestation inquiries
- Display pending rule violations
- Display pending policy violations
- Display your cases

The following tables provide you with an overview of the menu items and actions that can be run from here.

Table 62: Menu items

Menu	Menu item	Description
Information		
	Pending requests	Here you can display and approve pending requests (see Approving and denying requests on page 111).
	Request inquiries	Here you can display submitted request inquiries within the scope of an approval workflow (see Answering inquiries about

Menu	Menu item	Description
		requests on page 134).
	Pending attestations	Here you can display and approve attestation cases (see Pending attestations on page 177).
	Attestation inquiries	Here you can display submitted attestation inquiries within the scope of an approval workflow (see Attestation inquiries on page 189).
	Pending rule violations	Here you can display and approve pending rule violations (see Managing rule violations on page 201).
	Pending Policy Violations	Here you can display and approve pending policy violations (see Managing policy violations on page 205).
	My Processes	Here you can display processes that you initiated and are currently being processed.

My Processes (page description)

To open the **My Processes** page go to **(Information)** > **My Processes**.

On the **My Processes** page, you can display processes that you initiated and are currently being processed.

The following table gives an overview of the content of the **My Processes** page.

Table 63: Columns

Property	Description
Status	Shows the process status.
Process displays	Shows you which process is being run.
Created on	Shows you when the process was created/initiated.
Modified on	Shows you when the process was last changed.

My requests (Menu description)

Use the various menu items in the menu (**My Requests**) to perform the following actions:

- Request products from different service categories
- Manage your shopping cart

- Renew products
- Unsubscribe products

The following tables provide you with an overview of the menu items and actions that can be run here.

Table 64: Menu items

Menu	Menu item	Description
My requests		
	Request	Here you can request products from different service categories (see Requesting products on page 86).
	Shopping cart	You select the following actions: • Display and edit your shopping cart (see Managing products in the shopping cart on page 88) • Display and edit your Saved for Later list (see Saved for Later list on page 106)
	Renew or unsubscribe	You select the following actions: • Renew products (see Renewing products with limit validity periods on page 130) • Unsubscribe products (see Unsubscribing products on page 131) • Cancel active requests (see Canceling requests on page 129)

Profile (Menu description)

Use the (**Profile**) menu items to view and edit your own profile data, show the address book, or log out of the Web Portal. The following tables provide you with an overview of the menu items and actions that can be run here.

Table 65: Menu items

Menu	Menu item	Description
Profile		
	My Profile	Here you can manage various information about your user profile.
	Address book	You select the following actions: • Display all your company's identities (see Displaying the

Menu	Menu item	Description
		address book on page 51). • Display more information about identities (see Displaying the address book on page 51).
	Log Off	Use this to menu item log off from Web Portal (see Logging off on page 32).

My profile (page description)

To open the **My Profile** page go to (**<profile>**) > **My Profile**.

On the **My Profile** page, you can manage various information about your user profile.

To do this, click on one of the tiles:

Table 66: Tiles

Tiles	Description
Overview	Opens the **Overview - Identity** page (see Overview – Identity (page description) on page 848). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes.
Contact data	Opens the **Contact Data** page (see Contact data (page description) on page 848). Here you can: • Display and edit your personal data (see Editing your profile information on page 57) • Generate reports (see Creating reports about my identities on page 303)
Password	Opens the **Password Questions** page (see Password questions (page description) on page 850). Here you can manage your password questions (see Managing password questions on page 52).
Attestation	Opens the **Attestation – Identity** page (see My attestation status (page description) on page 897). You select the following actions: • Display pending attestation cases that you are involved in (see Displaying your attestation cases on page 175) • Grant or deny approval to attestation cases that you are involved

Tiles	Description
	in (see Granting or denying my attestation cases on page 176) • Send reminder emails to attestors (see Sending reminders for your own attestation cases on page 168)
Entitlements	Opens the **Entitlements – Identity** page (see Entitlements – Identity (page description) on page 851). Here you see the entitlements assigned to you.
Delegations	Opens the **Delegations – Identity** page (see Delegation (page description) on page 1170). You select the following actions: • Display all active delegations that you are involved in • Delegate your role memberships and responsibilities to other identities (see Adding delegations for my identities on page 307) • Delete delegations (see Deleting my identities' delegations on page 308) • Cancel delegations (see Deleting my identities' delegations on page 308)

Overview – Identity (page description)

To open the **Overview - Identity** page go to **(Profile)** > **My Profile** > **Overview**.

On the **Overview - Identity** page, you can view all the relevant information in your profile summarized in an overview.

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Contact data (page description)

To open the **Contact Data** page go to **(profile)** > **My Profile** > **Contact data**.

On the **Contact Data** page, you can:

- Display and change your contact and profile data (see Editing your profile information on page 57)
- Edit your Active Directory user accounts (see Editing Active Directory user accounts on page 57)
- Change the language in the Web Portal (see Switching languages on page 58)
- Change display and format values in the Web Portal (see Switching languages

on page 58)

- Generate reports (see Creating reports about my identities on page 303)

The following tables give you an overview of the various features and content on the **Contact Data** page.

Table 67: Controls

Control	Description
Generate report	Opens a dialog. Use this button to generate a report about your data (see Creating reports about my identities on page 303).
Save	Use this button to save the changes to the data.

You can change the following data.

Table 68: Contact data

Property	Description
Last name	Shows your last name.
First name	Shows your first name.
Default email address	Your default email address
Gender	In the menu, select your gender.
Manager	Shows your manager.
Primary cost center	Shows you which cost center you are primarily assigned to.
Primary department	Shows you which department you are primarily assigned to.
Primary location	Shows you which location you are primarily assigned to.
Room	Enter the room that you work in.
Street	Enter the street where you work.
Zip code	Enter the zip code of your place of work.
City	Enter the city where you work.
Country	Click **Assign/Change** and then select the country you work in.
Language	Click **Assign/Change** and then click the language in which you want to display the Web Portal.

Property	Description
Language for value formatting	Click **Assign/Change** and then click the language for date and number formats. For example, German dates are displayed in the format DD.MM.JJJJ (24.12.2020) and in English format MM/DD/JJJJ (12/24/2020).
Phone	Enter your phone number.
Mobile phone	Enter your mobile phone number.
Fax	Enter your fax number.
Image	Click **Change** and then select an image to use as your profile picture from your medium.

Password questions (page description)

To open the **Password Questions** page go to **(profile)** > **My Profile** > **Password**.

On the **Password Questions** page, you can:

- Create password questions (see Managing password questions on page 52)
- Edit password questions (see Managing password questions on page 52)
- Delete password questions (see Managing password questions on page 52)
- Unlock password questions (see Managing password questions on page 52)

The following tables give you an overview of the various features and content on the **Request Questions** page.

Table 69: Controls

Control	Description
Edit	Opens a dialog. Use this button to edit or delete a password question (see Managing password questions on page 52).
Unlock	Use this button to unlock a password question (see Managing password questions on page 52).
New question	Use this button to add a new password question (see Managing password questions on page 52).
Save	Use this button to save the changes to the password question.

Entitlements – Identity (page description)

To open the **Entitlements – Identity** page go to (**Profile**) > **My Profile** > **Entitlements**.

On the **Entitlements – Identity** page, you can display all entitlements assigned to you summarized in an overview.

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Address book

Open the **Address Book** page through the (**profile**) > **Address Book** menu item (see Displaying the address book on page 51).

On the**Adress Book** page, you can:

- Display all your company's identities (see Displaying the address book on page 51)
- Display more information about identities (see Displaying the address book on page 51)

The following tables give you an overview of the different functions and content on the **Address Book** page.

Table 70: Controls in the details pane of an identity

Control	Description
Overview	You can use this button to display more information about the identity.

Table 71: Columns

Column	Description
Display	Displays the full name and in brackets, the user name of the employee.
Primary location	Shows the identity's primary location.
Primary department	Shows the department that the identity is primarily assigned to.

Help (Menu description)

Use the various menu items in the menu (**Help**) to perform the following actions:

- Open One Identity help resources
- General information about the Web Portal
- Change the user interface language
- Change the user interface time zone

The following tables provide you with an overview of the menu items and actions that can be run here.

Table 72: Menu items

Menu	Menu item	Description
Help		
	Help	Opens the Web Portal's context-sensitive help.
	Support	Opens the One Identity's support page. There you will find a number of solution methods for different issues.
	Community	Opens One Identity's community page, where you can exchange solutions with other users in a forum.
	Connection	Here you can display detailed information about the logged-in user, authorization groups, and program functions.
	Info	Here you can display, among other things, information about the currently installed version of your Web Portal and legal notices of the product.
	Language	Here you can change the Web Portal's display language (see also Switching languages on page 58).
	Time zones	Here you can change the Web Portal's time zone.

Request (Menu description)

You can use items on the **Request** menu to perform various actions and collect information about requests. The following tables provide you with an overview of the menu items and actions that can be run here.

Table 73: Menu items

Menu	Menu item		Description
Request			
	My requests		
		New	Here you can add products that you want to request into

Menu	Menu item		Description
		Request	your shopping cart (see Adding products to the shopping cart on page 87).
		Request history	You select the following actions: • Display products that you have requested or other identities have requested for you (see Displaying request history on page 128) • Resubmit requests (see Resubmitting requests on page 128) • Cancel requests (see Canceling requests on page 129) • Revoke approval delegations (see Withdrawing delegations from pending requests on page 121) • Release requests for approval (see Revoking hold status of pending requests on page 127) • Withdraw additional approval (see Removing additional approvers of pending requests on page 120) • Recall last question asked (see Deleting inquiries about pending requests on page 126)
		Editing requests	You select the following actions: • Extend the validity period of products (see Renewing products with limit validity periods on page 130) • Unsubscribe products (see Unsubscribing products on page 131) • Cancel active requests (see Canceling requests on page 129) • Escalate request approvals
		Maintaining templates	Here you can perform the following actions for your own or system-wide request templates: • Show request templates (see Displaying request templates on page 81) • Create request templates (see Creating request templates on page 82) • Share request templates with other identities (see Sharing request templates on page 85) • Edit request templates (see Editing request

Menu	Menu item		Description
			templates on page 83) • Delete request templates (see Deleting request templates on page 85)
		Shopping cart	You select the following actions: • Display your shopping cart (see Displaying the shopping cart on page 89) • Manage your shopping cart (Managing products in the shopping cart on page 88) • Display your saved for later list (see Displaying Saved for Later list on page 107) • Manage your saved for later list (see Saved for Later list on page 106)
	My actions		
		Pending requests	You select the following actions: • Display all requests that you can approve (see Displaying pending requests on page 111) • Grant or deny requests (see Approving and denying requests on page 111) • Make inquiries about requests if the information is insufficient to make an approval decision (see Sending inquiries about pending requests on page 125) • Add other approvers that can approve requests (see Appointing additional approvers to pending requests on page 120) • Reroute request approvals to other identities (see Rerouting approvals of pending requests on page 119) • Delegate request approvals to other identities (see Delegating approvals of pending requests to other identities on page 121) • Pass request approvals to the fallback approver or the chief approval team (see Escalating approvals of pending requests on page 122) • Change the priority of requests (see Changing priority of pending requests on page 123) • Confirm terms of use of products requested for you (see Confirming terms of use on page 124)

Menu	Menu item		Description
			• Add more products to existing requests (see Adding more products to pending requests on page 124) • Cancel requests (see Canceling pending requests on page 125) • Revoke requests' hold status (see Revoking hold status of pending requests on page 127)
		Approval history	You select the following actions: • Display all approvals of product requests that you, or the identities that report to you, decided upon (see Displaying approvals on page 132) • Cancel requests (see Canceling requests on page 129) • Revoke approval delegations (see Withdrawing delegations from pending requests on page 121) • Release requests for approval (see Revoking hold status of pending requests on page 127) • Withdraw additional approval (see Removing additional approvers of pending requests on page 120)
		Request inquiries	You select the following actions: • Display questions that you were asked about certain requests (see Displaying request inquiries on page 133) • Answer questions that you were asked about certain requests (see Answering inquiries about requests on page 134)
	Auditing		
		Request	Here you can see all the requests. You can also filter them so that only products requested for a specific identity are displayed (see Displaying all requests on page 135).
		Approval	Here you can see all the approvals. You can also filter them so that only requests relating to a specific identity are displayed (see Displaying all approvals on page 136).
	Escalation		You select the following actions:

Menu	Menu item	Description
		• Display all escalated requests that you can approve (see Displaying escalated requests on page 137) • Grant or deny requests (see Approving and denying escalated requests on page 138) • Make inquiries about requests if the information is insufficient to make an approval decision (see Submitting inquiries about escalated requests on page 150) • Add other approvers that can approve requests (see Appointing additional approvers to escalated requests on page 146) • Reroute request approvals to other identities (see Rerouting escalated requests' approvals on page 145) • Delegate request approvals to other identities (see Delegating approvals of escalated requests to other identities on page 147) • Change the priority of requests (see Changing priority of pending requests on page 123) • Add more products to existing requests (see Adding more products to escalated requests on page 149) • Cancel requests (see Canceling escalated requests on page 150) • Revoke requests' hold status (see Revoking hold status of escalated requests on page 152)

My requests (page description)

Open the **Pending Request** page, by navigating through to **Request** > **My Requests**.

On the **My Requests** page you can perform various actions regarding your requests. To do this, click on one of the tiles:

Table 74: Tiles

Tiles	Description
New Request	Here you can add products that you want to request into your shopping cart (see Adding products to the shopping cart on page 87).

Tiles	Description
Request history	You select the following actions: • Display products that you have requested or other identities have requested for you (see Displaying request history on page 128) • Resubmit requests (see Resubmitting requests on page 128) • Cancel requests (see Canceling requests on page 129) • Revoke approval delegations (see Withdrawing delegations from pending requests on page 121) • Release requests for approval (see Revoking hold status of pending requests on page 127) • Withdraw additional approval (see Removing additional approvers of pending requests on page 120) • Recall last question asked (see Deleting inquiries about pending requests on page 126)
Editing requests	You select the following actions: • Extend the validity period of products (see Renewing products with limit validity periods on page 130) • Unsubscribe products (see Unsubscribing products on page 131) • Cancel active requests (see Canceling requests on page 129) • Escalate request approvals
Maintain-ing templates	Here you can perform the following actions for your own or system-wide request templates: • Show request templates (see Displaying request templates on page 81) • Create request templates (see Creating request templates on page 82) • Share request templates with other identities (see Sharing request templates on page 85) • Edit request templates (see Editing request templates on page 83) • Delete request templates (see Deleting request templates on page 85)
Shopping cart	You select the following actions: • Display your shopping cart (see Displaying the shopping cart on page 89) • Manage your shopping cart (Managing products in the shopping cart on page 88)

Tiles	Description
	• Display your saved for later list (see Displaying Saved for Later list on page 107) • Manage your saved for later list (see Saved for Later list on page 106)

Request (page description)

To open the **Request** page go to **Request** > **My Requests** > **Start a new request**.

On the **Request** page, you can add products that you want to request to your shopping cart (see Adding products to the shopping cart on page 87).

There are products in the list that are marked with an icon. The meanings of these icons are explained in the table below with relevance to the product.

Table 75: Request status

Icon	State
	The product was requested and is already assigned. You cannot make another request at the moment.
	The product was already requested or it is not currently available. It cannot be requested at the moment.
	A pending request already exists for this product. You cannot repeat the request at the moment.
	The product was already assigned to the user. NOTE: The product assignments can be inherited, for example. It is not possible to make another request for this product. If the request is repeated, the status changes to **This product has already been requested**.

The following tables give you an overview of the various features and content on the **Request** page.

Table 76: Controls

Control	Description
Recipient	Shows you the identity for whom you are selecting products. Use the **Change** button to select for which identities you want to request the products (see Requesting for other identities or subidentities on page 98).
Find a service item	Use this search to help you find the products you want to request.

Control	Description
Service items in the category	Shows you to which service category the displayed products belong. If the service category contains subcategories, click in the list and select the appropriate subcategory.
Change service category	Use this button to select another service category.
Include child categories	Use this check box to group together main and subcategories of the selected service category in a list.
Add to cart	This opens the **My Shopping Cart** page (see My shopping cart (page description) on page 869). Use this button to add all the products you have selected using the (**Add to cart**) check box next to the product to the shopping cart (see Adding products to the shopping cart on page 87).
Actions > Check requests for this recipient	This opens the **Requests for <identity>** page (see Requests for identities (page description) on page 860). Use this action to check which products the selected recipient already owns. This prevents you from requesting products that the recipient already has.
Actions > Select a request template	Use this action to request products from a request template (see Requesting using request templates on page 101).
Actions > Select a reference user	Use this action to request products that a specific identity already has (see Requesting products through reference users on page 100).
Actions > Show products other identities requested	This opens the **Products other identities requested** page (see Products other identities requested (page description) on page 861). Use this action to display and request products that other identities in the system have already requested (see Requesting products through peer groups on page 100).

Table 77: Columns

Column	Description
Add to cart	Select the check box next to the product you want to add to the shopping cart. Then, using the **Add to cart** button, add these products to the shopping cart (see Adding products to the shopping cart on page 87).
Product	Shows you the product's name.
Service category	Shows you to which service category the product belongs.
Request	Use the **Add to cart** button to add the corresponding product to the shopping cart (see Adding products to the shopping cart on page 87).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: You can see more information about each action in the details pane. In the list, click the corresponding product and expand the details pane by clicking on the gray area.

Requests for identities (page description)

To open the **Requests for <identity>** page go to **Request** > **My Requests** > **Start a new request** > **Actions** > **Select a reference user**.

On the **Requests for <identity>** page, you display and request products that a previously selected identity has already request (see Requesting products through reference users on page 100). This way, you have a quick method of requesting products that are important to you or your identities.

There are products in the list that are marked with an icon. The meanings of these icons are explained in the table below with relevance to the product.

Table 78: Request status

Icon	State
	The product was requested and is already assigned. You cannot make another request at the moment.
	The product was already requested or it is not currently available. It cannot be requested at the moment.
	A pending request already exists for this product. You cannot repeat the request at the moment.
	The product was already assigned to the user. NOTE: The product assignments can be inherited, for example. It is not possible to make another request for this product. If the request is repeated, the status changes to **This product has already been requested**.

The following tables give you an overview of the various features and content on the **Requests for <identity>** page.

Table 79: Controls

Control	Description
Add to cart	Use this button to add to the shopping cart all the products you have selected using the check box next to the product in the **Request** column.
Create template	Use this button to create a request template that you can reuse later to save time (see Creating request templates on page 82).

Table 80: Columns

Column	Description
Request	Select the check box next to the product you want to add to the shopping cart. Then, using the **Add to cart** button, you can add these products to the shopping cart.
Full name	Shows you the product's name.
Description	Shows you the description of the product.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Products other identities requested (page description)

To open the **Products other identities requested** page go to **Request** > **My Requests** > **Start a new request** > **Actions** > **Show products other identities requested**.

On the **Products other identities requested** page, you can display and request products that other identities in the system have already requested (see Requesting products through peer groups on page 100). As a manager, you can also see products from the peer group of an identity that you manage. This way, you have a quick method of requesting products that are important to you or your responsible identities.

TIP: A peer group contains all the identities that have the same manager or the same primary or secondary department as the request recipient.

There are products in the list that are marked with an icon. The meanings of these icons are explained in the table below with relevance to the product.

Table 81: Request status

Icon	State
	The product was requested and is already assigned. You cannot make another request at the moment.
	The product was already requested or it is not currently available. It cannot be requested at the moment.
	A pending request already exists for this product. You cannot repeat the request at the moment.
	The product was already assigned to the user. NOTE: The product assignments can be inherited, for example. It is not possible to make another request for this product. If the request is repeated, the status changes to **This product has already been requested**.

The following tables give you an overview of the various features and content on the **Products other identities requested** page.

Table 82: Controls

Control	Description
Add to cart	Use this button to add all the products you have selected using the (**Add to cart**) check box next to the product to the shopping cart.

Table 83: Columns

Column	Description
Selection	Select the check box next to the product you want to add to the shopping cart. Then, using the **Add to cart** button, you can add these products to the shopping cart.
Product	Shows you the product's name.
Number of identities	Shows you how many the peer group identities already own this product.
Distribution in the peer group	Shows you how many peer identities already own this product in percent.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Request history (page description)

To open the **Request History** page go to **Request** > **My Requests** > **Request History** (see Displaying request history on page 128).

On the **Request History** page, you can:

- Display products that you have requested or other identities have requested for you (see Displaying request history on page 128)
- Resubmit requests (see Resubmitting requests on page 128)
- Cancel requests (see Canceling requests on page 129)
- Revoke approval delegations (see Withdrawing delegations from pending requests on page 121)
- Release requests for approval (see Revoking hold status of pending requests on page 127)
- Withdraw additional approval (see Removing additional approvers of pending requests on page 120)
- Recall last question asked (see Deleting inquiries about pending requests on page 126)

The following tables give you an overview of the various features and content on the **Request History** page.

Table 84: Controls

Control	Description
Advanced search	The advanced search allows you to control which product requests are displayed (see Displaying request history on page 128): • **Requests submitted by you for yourself**: Select this check box to display product requests you placed yourself. • **Requests submitted by you for others**: Select this check box to display product requests you placed for other identities. • **Requests submitted by others for you**: Select this check box to display product requests other identities placed for you. • **Requests submitted by other users**: Select this check box to display product requests placed by other identities that report to you. • **Filter by request number**: Enter the request number of the request you want to display. • **pending**: Select this check box to display product requests that are not yet approved (status: **Request**). • **Approved**: Select this check box to display product requests that have been granted approval (status: **Assigned**). • **Canceled or denied or unsubscribed**: Select this check box to display product requests that have been canceled, denied, or unsubscribed (state: **Canceled**, **Denied**, **Unsubscribed**). Click **Search** to apply the filter criteria to the request history. Click **Reset** to reset the filter criteria to the default search.

Table 85: Controls in the details pane of a product

Control	Description
Submit again	Use this button to request the product again (see Resubmitting requests on page 128). After you enter a reason, the product will be added to your shopping cart and you can submit the request (see Submitting requests on page 97).
Cancel	Use this button to withdraw the selected product request (see Canceling requests on page 129). The button is only displayed if the product has the status **Request**.
Recall last question	Use this button to recall the question that you asked another identity about the product request (see Deleting inquiries about pending requests on page 126).
Withdrawing	Use this button to withdraw the delegation of the approval (see

Control	Description
delegation	Withdrawing delegations from pending requests on page 121). To do this, the request approval must have been transferred to another identity beforehand (see Delegating approvals of pending requests to other identities on page 121).
Withdrawing additional approval	If you have appointed an additional approver for this product request (see Appointing additional approvers to pending requests on page 120), use this button to revoke the action. Then you are the only approver of this product request (see Removing additional approvers of pending requests on page 120).
Revoking hold status	Use this button to release the request for approval again so that it can be processed by the approvers (see Revoking hold status of pending requests on page 127).

Table 86: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product request (see Approving and denying requests on page 111). The following status' are possible: • **Assigned**: The product request was successful and the product was successfully assigned. • **Request**: The product request is still awaiting an approval decision (it is still in the request workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The product request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The product request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Renewal**: The product has been renewed (see Renewing products with limit validity periods on page 130). • **Unsubscription**: The product is being unsubscribed (see Unsubscribing products on page 131). • **Denied**: The request for this product was denied. The reason for denying may be a policy or rule violation or the manager not verifying the request if it is only temporary. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. . • **Canceled**: The product request was canceled (see Canceling requests

Column	Description
	on page 129) or the system could not carry out the request (for example, because an identity for verifying it was not given or the validity period expired). In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed**: The product was unsubscribed (see Unsubscribing products on page 131). In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows you the request number of the total request with which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Renewing or unsubscribing (page description)

To open the **Renew or renew** page go to **Request** > **My Requests** > **Edit Requests**.

On the **Renew or Unsubscribe** page, you can:

- Extend the validity period of products (see Renewing products with limit validity periods on page 130)
- Unsubscribe products (see Unsubscribing products on page 131)
- Cancel active requests (see Canceling requests on page 129)
- Escalate request approvals

The following tables give you an overview of the various features and content on the **Renew or Unsubscribe** page.

Table 87: Controls

Control	Description
Requests for	Shows you the identity whose products you are displaying. Use the **Change** button to select whose products you want to display.
Unsubscribe	Use this button to unsubscribe the selected product (see Unsubscribing products on page 131).
Renew	Use this button to renew the validity period of the selected product (see Renewing products with limit validity periods on page 130).

Table 88: Controls in the details pane of a product

Control	Description
Escalate request	Use this button to escalate the product request. If the approver responsible is not available for an extended period or has no access to Web Portal, then the fallback approver or member of the chief approval team can make an approval decision. The button is only displayed if the product can be escalated. For more information, see Escalated requests on page 137.
Show request	Opens the **Request overview** page (see Request overview ((page description)) on page 867). Use this button to display the entire request used to request this product.
Withdraw request	Use this button to withdraw the selected product request (see Canceling requests on page 129). The button is only displayed if the product has the status **Request**.

Table 89: Columns

Column	Description
Valid until	Shows you when product expires.
Product	Shows you the product's name.
State	Shows the current status of the product. The following status' are possible: • **Assigned**: The request was successful and the product was successfully assigned to you. • **Request**: The request is still awaiting an approval decision (it is still in the workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Unsubscription**: The product is being unsubscribed. In the details pane, on the **Workflow** tab, you can see the current position in the workflow.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Request overview ((page description))

To open the **Request Overview** page go to **Request** > **My Requests** > **Edit Requests** > Details pane > **Show request** (see Displaying and approving entire requests of pending requests on page 113).

The **Request overview** page provides an overview of all the products from a specific request.

The following table gives you an overview of the different functions on the **Request overview** page.

Table 90: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product. The following status' are possible: • **Assigned**: The request was successful and the product was successfully assigned. • **Request**: The request is still awaiting an approval decision (it is still in the workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Renew**: The product was just renewed. • **Unsubscription**: The product is being unsubscribed. • **Deny**: The request was denied. In the details pane, on the **Workflow** tab, you can see when and why the request was denied.

Column	Description
	• **Canceled**: The request was canceled. In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Canceled**: The request was canceled. In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested.
Recipient	Shows for whom the product was requested.
Shopping cart	Show the request shopping cart from which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Shopping Cart Templates (page description)

To open the **Cart Templates** page go to **Request** > **My Requests** > **Maintain Templates** (see Displaying request templates on page 81).

On the **Cart Templates** page you can perform the following actions for your own or system-wide request templates:

- Show request templates (see Displaying request templates on page 81)
- Create request templates (see Creating request templates on page 82)
- Share request templates with other identities (see Sharing request templates on page 85)
- Edit request templates (see Editing request templates on page 83)
- Delete request templates (see Deleting request templates on page 85)

For more information about requesting from an request template, see Requesting using request templates on page 101.

The following table gives you an overview of the various features on the **Cart Templates** page.

Table 91: Controls

Control	Description
Expand	Use this button to display the contents of the request template.
Edit	You can use this button to add additional information to the request template (see) or share the request template with other identities (see Sharing request templates on page 85).
Delete	You can use this button to delete the request template (see Deleting request templates on page 85) or remove individual products from the template (see Removing products from request templates on page 84).

Table 92: Templates – status

Status	Meaning
	This template has not been approved yet. A decision about publishing it still pending.
	The template is marked for public use but was not published yet.
	The template has been released for publication and can be used by other identities.

My shopping cart (page description)

To open the **My shopping cart** page go to **Request** > **My requests** > **Shopping cart** (see Displaying the shopping cart on page 89).

When you select products for a request, first they are added to the shopping cart and displayed on the **My Shopping Cart** page. Once you have placed all the products in the shopping cart, you can send the requests. If you want request products at a later date, you can move them from here to the Saved for later list (see Saving products for later on page 107).

To find out how to manage products in the shopping cart, see Managing products in the shopping cart on page 88.

NOTE: In certain circumstances, you may cause a compliance violation when you grant approval to a request, which allocates a specific entitlement to a business role. For example, this might occur if an identity obtains an unauthorized entitlement through this business role. In this case, the compliance violation is displayed in the details pane of the shopping cart.

On the **My Shopping Cart** page, you can:

- Display your shopping cart (see Displaying the shopping cart on page 89)
- Manage your shopping cart (Managing products in the shopping cart on page 88)

- Display your saved for later list (see Displaying Saved for Later list on page 107)
- Manage your saved for later list (see Saved for Later list on page 106)

The following tables give you an overview of the various features and content on the **My Shopping Cart** page.

Table 93: Controls

Control	Description
Actions > Check shopping cart	Use this action to check the requests in the shopping cart (see Checking the shopping cart and removing invalid products on page 95). After checking, you will know whether the request can be carried out.
Actions > Create template from shopping cart	This opens the **Cart Templates** page. Use this action to create a template from the shopping cart to create further requests (see Creating request templates on page 82). For example, you can use this template for another recipient (see Requesting using request templates on page 101).
Actions > Delete invalid requests	Use this action to remove requests from the shopping cart that have either violate a rule or have insuffient permissions (see Checking the shopping cart and removing invalid products on page 95).
Actions > Delete shopping cart	Use this action to empty the entire shopping cart (see Deleting shopping carts on page 97).
Actions > View Saved for Later list	This opens the **Saved for Later** page (see Saved for Later list (page description) on page 871). Use this action to show your Saved for later list (see Displaying Saved for Later list on page 107).
Actions > Edit details	This opens the Details page (see Details (page description) on page 873). Use this action to edit multiple products in the shopping cart and apply the changes to them all (see Editing multiple products in the shopping cart on page 90).
Edit	Use this action to: • Specify the validity period of all products in the shopping cart (see Setting the validity period of products in your shopping cart on page 91) • Enter a reason for requesting all products (see Giving reasons for requests on page 93)
Submit	Use this button to check the request and submit it (see Submitting requests on page 97).

Table 94: Controls in the details pane of a product

Control	Description
	This symbol shows the current information about the product. In some cases, this icon is available as an action on the product if a request with dependent products cannot be sent.
Delete	Use this button to delete the product from the shopping cart (see Removing products from the shopping cart on page 90).
Save	Use this button to save information that you have edited in the product's details pane.
Actions > Request for multiple identities	Use this action to duplicate requests in the shopping cart for other identities (see Requesting products in the shopping cart for multiple identities on page 96).
Actions > Save for later	Use this action to move requests from the shopping car to the Saved for Later list (see Saving products for later on page 107).

Table 95: Columns

Column	Description
Request	Shows you the name of the product you want to request
Recipient	Shows for whom the product is requested.
Status	Shows you if the product can be requested or if there are problems. The status is displayed only after the request has been checked for validity (see Checking the shopping cart and removing invalid products on page 95).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: You can make further settings for each product in the details pane. To do this, click the product in the list:

Saved for Later list (page description)

To open the **Saved for Later** page go to **Request** > **My Requests** > **Shopping Cart** > **Actions** > **View Saved for Later list** (see Displaying Saved for Later list on page 107)

On the **Saved for Later** list, you can:

- Display all products that you have saved for requesting later (see Displaying Saved for Later list on page 107)
- Move products from the Saved for Later list to the shopping cart to request them (see Requesting products on the Saved for Later list on page 108)

- Remove products from the Saved for Later list (see Removing products from the Saved for Later list on page 109)
- Delete the entire Saved for Later list (see Deleting the Saved for Later list on page 110)

TIP: To find out how to save a product for later, see Saving products for later on page 107.

The following tables give you an overview of the various features and content on the **Saved for Later** page.

Table 96: Controls

Control	Description
Deleting the Saved for Later list	Use this button to delete the entire Saved for Later list (see Deleting the Saved for Later list on page 110).
Delete selected	Use this button to remove all the products from shopping cart you selected using the check box next to the product in the **Select** column (see Removing products from the Saved for Later list on page 109).
Move to shopping cart	Use this button to move to the shopping cart all the products you have selected using the check box next to the product in the **Select** column (see Requesting products on the Saved for Later list on page 108).

Table 97: Controls in the details pane of a product

Control	Description
Delete	Use this button to delete the product from the Saved for Later list (see Removing products from the Saved for Later list on page 109).
Save	Use this button to save additional information about the product in the details pane.
Actions > Move to shopping cart	Use this action to move request from the Saved for Later list to the shopping cart and request them there (see Requesting products on the Saved for Later list on page 108).

Table 98: Columns

Column	Description
Select	Select the check box next to the products you want to move to the shopping cart or delete from the Saved for Later list. Then, using the **Move to shopping cart** or **Delete selected** buttons, you can move these products to the shopping cart or delete them from the Saved for Later list.
Request	Shows you the name of the product you want to request
Recipient	Shows you for whom the product is requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: You can make further settings for each product in the details pane. To do this, click the product in the list:

Details (page description)

To open the **Details** page go to **Request** > **My Requests** > **Shopping Cart** > **Actions** > **Edit details**.

If you have several products in the shopping cart, you can edit them individually on the **Details** page and apply modified properties to several of the same products. This way, you do not have to adjust the same settings separately for each individual product, but can "copy" the changes (see Editing multiple products in the shopping cart on page 90).

The following tables give you an overview of the various features and content on the **Details** page.

Table 99: Controls

Control	Description
Apply to all	Use this button to apply changes made in the field next to it to all other products of the same type (see Editing multiple products in the shopping cart on page 90).
Save	Use this button to save all the changes.

Table 100: Columns

Column	Description
Recipient	Shows you for whom the product is requested.
Settings	Shows you all the data you can change.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

My actions (page description)

To open the **My Actions** page go to **Request** > **My Actions**.

On the **My Actions** page, you can perform various actions for requests in which you are involved as an approver.

To do this, click on one of the tiles:

Table 101: Tiles

Tile	Description
Pending requests	You select the following actions: • Display all requests that you can approve (see Displaying pending requests on page 111) • Grant or deny requests (see Approving and denying requests on page 111) • Make inquiries about requests if the information is insufficient to make an approval decision (see Sending inquiries about pending requests on page 125) • Add other approvers that can approve requests (see Appointing additional approvers to pending requests on page 120) • Reroute request approvals to other identities (see Rerouting approvals of pending requests on page 119) • Delegate request approvals to other identities (see Delegating approvals of pending requests to other identities on page 121) • Pass request approvals to the fallback approver or the chief approval team (see Escalating approvals of pending requests on page 122) • Change the priority of requests (see Changing priority of pending requests on page 123) • Confirm terms of use of products requested for you (see Confirming terms of use on page 124) • Add more products to existing requests (see Adding more products to pending requests on page 124) • Cancel requests (see Canceling pending requests on page 125) • Revoke requests' hold status (see Revoking hold status of pending requests on page 127)
Approval history	You select the following actions: • Display all approvals of product requests that you, or the identities that report to you, decided upon (see Displaying approvals on page 132) • Cancel requests (see Canceling requests on page 129) • Revoke approval delegations (see Withdrawing delegations from pending requests on page 121) • Release requests for approval (see Revoking hold status of pending requests on page 127) • Withdraw additional approval (see Removing additional approvers of pending requests on page 120)

Tile	Description
Request inquiries	You select the following actions: • Display questions that you were asked about certain requests (see Displaying request inquiries on page 133) • Answer questions that you were asked about certain requests (see Answering inquiries about requests on page 134)

Pending attestations (page description)

Open the **Pending Request** page, by navigating through to **Request** > **My actions** > **Pending requests.**

Many requests go through a manual approval process in order to ensure the correct assignment of products. For more information about requests, see Pending requests on page 110.

On the **Pending Attestations** page, you can:

- Display all requests that you can approve (see Displaying pending requests on page 111)
- Grant or deny requests (see Approving and denying requests on page 111)
- Make inquiries about requests if the information is insufficient to make an approval decision (see Sending inquiries about pending requests on page 125)
- Add other approvers that can approve requests (see Appointing additional approvers to pending requests on page 120)
- Reroute request approvals to other identities (see Rerouting approvals of pending requests on page 119)
- Delegate request approvals to other identities (see Delegating approvals of pending requests to other identities on page 121)
- Pass request approvals to the fallback approver or the chief approval team (see Escalating approvals of pending requests on page 122)
- Change the priority of requests (see Changing priority of pending requests on page 123)
- Confirm terms of use of products requested for you (see Confirming terms of use on page 124)
- Add more products to existing requests (see Adding more products to pending requests on page 124)
- Cancel requests (see Canceling pending requests on page 125)
- Revoke requests' hold status (see Revoking hold status of pending requests on page 127)

The following tables give you an overview of the different functions and content on the **Attestations** page.

Table 102: Controls

Control	Description
Approve	Use this button to approve the product request (see Approving and denying requests on page 111).
Deny	Use this button to deny the product request (see Approving and denying requests on page 111).
Approve all	Use this button to approve the all the product requests shown (see Approving and denying requests on page 111).
Deny all	Use this button to deny the all the product requests shown (see Approving and denying requests on page 111).
Next	Opens the **Pending Requests – Approvals** (see Pending requests – Approvals on page 880). Use this button to show an overview of all approvals made that you still make adjustments to and then save. As long as you have not made an approval decision (by using the appropriate button), this button is disabled.

Table 103: Controls in the details pane of a product

Control	Description
Withdraw request	Use this button to approve the product request (see Canceling pending requests on page 125.
Revoking hold status	Use this button to release the request for approval again so that it can be processed by the approvers (see Revoking hold status of pending requests on page 127).
Withdrawing additional approval	If you have appointed an additional approver for this product request (see Appointing additional approvers to pending requests on page 120), use this button to revoke the action. Then you are the only approver of this product request (see Removing additional approvers of pending requests on page 120).
Recall last question	Use this button to recall the question that you asked another identity about the product request (see Deleting inquiries about pending requests on page 126).
Display the identity's entitlements	Use this button to specify which modifications to make to the effective date of change (see Approving new managers' pending requests on page 117).
more > Send inquiry	Use this function to send an inquiry to an identity about the product request (see Sending inquiries about pending requests on page 125).
more > Show entire request	Use this action to show the entire request that was used to request this product (see Displaying and approving entire requests of pending requests on page 113).

Control	Description
more > Reroute approval	Use this action to let another approval level make the approval decision about a product. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending requests on page 119).
more > Add approver	Use this action to add an additional approver to share the approval decision about the request (see Appointing additional approvers to pending requests on page 120). You can revoke this action in the approval history (see Removing additional approvers of pending requests on page 120).
more > Delegate approval	Use this action to delegate the approval decision about the request to another identity (see Delegating approvals of pending requests to other identities on page 121)(see Delegating approvals of escalated requests to other identities on page 147).
more > Reject approval	Use this action to reject the product request (see Rejecting request approval on page 122). The approval decision is returned to the original approver.
more > Escalate approval	Use this action to escalate the approval of this product request such that a fallback approver or member of the chief approval team can make the approval decision for this request (see Escalating approvals of pending requests on page 122).
more > Change priority	Use this action to change the priority of the product request (see Changing priority of pending requests on page 123).

Table 104: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product.
Request date	Shows when the product was requested.
Recipient	Shows for whom the product was requested.
Priority	Shows the priority for this product request.
Approval	Use these two buttons to make an approval decision about the product request. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Requests overview (page description)

To open the **Request overview** page go to **Request** > **My Actions** > **Pending Requests** > Details pane > **more** > **Show entire request**.

The **Request overview** page provides an overview of all the products from a specific request and you can approve all the pending product requests (see Displaying and approving entire requests of pending requests on page 113).

The following tables give you an overview of the different functions and content on the **Request overview** page.

Table 105: Controls

Control	Description
Add items to this request	Opens the **Request** page (see Request (page description) on page 858). Use this button to add more products to the corresponding request (see Adding more products to pending requests on page 124).
Approve all	Opens the **Pending Requests – Approvals** (see Pending requests – Approvals on page 880). Use this button to approve all pending product requests in this request (see Displaying and approving entire requests of pending requests on page 113.

Table 106: Controls in the details pane of a product

Control	Description
Cancel	Use this button to cancel the product request (see Canceling pending requests on page 125).

Table 107: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product.

Column	Description
	The following status' are possible: • **Assigned**: The request was successful and the product was successfully assigned. • **Request**: The request is still awaiting an approval decision (it is still in the workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Renew**: The product was just renewed. • **Unsubscription**: The product is being unsubscribed. • **Deny**: The request was denied. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. • **Canceled**: The request was canceled. In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed**: The request was unsubscribed. In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows the request shopping cart from which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Pending requests – Approvals

To open the **Pending Requests – Approvals** page go to **Request** > **My Actions** > **Pending Requests** > Make approval decision > **Next**.

After you have made your approval decisions on the **Pending Requests** page, you can save the approval on the **Pending Requests – Approvals** page so that they take effect (see Approving and denying requests on page 111). You can also enter reason for the approval decisions here.

The following tables give you an overview of the different functions and content on the **Pending Requests – Approvals** page.

Table 108: Controls

Control	Description
Reason for approvals	Here you can enter a reason for all approved product requests.
Standard reason	Here you can select one of the standard reasons saved in the system for all approved product requests.
Reason for denials	Here you can enter a reason for all denied product requests.
Standard reason	Here you can select one of the standard reasons saved in the system for all denied product requests.
Save	Use this button to save all the settings and approval decisions.
Back	Use this button to switch to the previous page. For example, to approve other product requests.

Table 109: Columns

Column	Description
Product	Shows the name of the product that was requested.
Recipient	Shows for whom the product was requested.
Valid from	Here you can specify from when the product is valid (see Changing priority of pending requests on page 123).
Valid until	Here you can specify until when the product is valid (see Changing priority of pending requests on page 123).
Reason	Here you can enter a reason for the decision. To do this, click on the link and, in the dialog, enter a reason or select one of the standard reasons.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Approval history (page description)

To open the **Approval history** page go to **Request** > **My actions** > **Pending requests** (see Displaying approvals on page 132).

On the **Approval History** page, you can:

- Display all approvals of product requests that you, or the identities that report to you, decided upon (see Displaying approvals on page 132)
- Cancel requests (see Canceling requests on page 129)
- Revoke approval delegations (see Withdrawing delegations from pending requests on page 121)
- Release requests for approval (see Revoking hold status of pending requests on page 127)
- Withdraw additional approval (see Removing additional approvers of pending requests on page 120)

If you only want to display approvals for a specific time period, use the filter function in the **Request date** column.

The following tables give you an overview of the various features and content on the **Approval History** page.

Table 110: Controls

Control	Description
Advanced search	The advanced search allows you to control which approvals are displayed: • **Approved by**: Click **Assign** and select the identity whose approvals you want to display. • **Filter by request number**: Enter the request number of the request you want to display. TIP: To find out the request number of a request, open the request history (see Displaying request history on page 128) and take the request number from the **Shopping Cart** column in the row of the corresponding product. • **Pending**: Select this check box to display product requests that you have made an approval decision about but have not yet been approved (status: **Request**). • **Approved**: Select this check box to display product requests that have been granted approval (status: **Assigned**). • **Canceled or denied or unsubscribed**: Select this check box to display product requests that have been canceled, denied, or unsubscribed (state: **Canceled**, **Denied**, **Unsubscribed**). Click **Search** to apply the filter criteria to the request history.

Control	Description
	Click **Reset** to reset the filter criteria to the default search.

Table 111: Controls in the details pane of a product

Control	Description
Withdraw request	Use this button to withdraw the product request Canceling requests on page 129.
Withdrawing delegation	Use this button to withdraw the delegation of the approval (see Withdrawing delegations from pending requests on page 121). To do this, the request approval must have been transferred to another identity beforehand (see Delegating approvals of pending requests to other identities on page 121).
Withdrawing additional approval	If you have appointed an additional approver for this product request (see Appointing additional approvers to pending requests on page 120), use this button to revoke the action. Then you are the only approver of this product request (see Removing additional approvers of pending requests on page 120).
Revoking hold status	Use this button to release the request for approval again so that it can be processed by the approvers (see Revoking hold status of pending requests on page 127).
Revoke last decision	Use this option to undo the last approval decision you made about this request.

Table 112: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product. The following status' are possible: • **Assigned**: The product request was successful and the product was successfully assigned. • **Request**: The product request is still awaiting an approval decision (it is still in the request workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The product request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The product request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow.

Column	Description
	• **Renewal**: The product has been renewed (see Renewing products with limit validity periods on page 130). • **Unsubscription**: The product is being unsubscribed (see Unsubscribing products on page 131). • **Denied**: The request for this product was denied. The reason for denying may be a policy or rule violation or the manager not verifying the request if it is only temporary. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. • **Canceled**: The product request was canceled or the system could not carry out the request (for example, because an identity for verifying it was not given or the validity period expired). In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed**: The product was unsubscribed (see Unsubscribing products on page 131). In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows you the request number of the total request with which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Request inquiries (page description)

To open the **Request Inquiries** page go to **Request** > **My Actions** > **Request Inquiries** (see Displaying request inquiries on page 133).

On the **Request Inquiries** page, you can:

- Display questions that you were asked about certain requests (see Displaying request inquiries on page 133)
- Answer questions that you were asked about certain requests (see Answering inquiries about requests on page 134)

The following tables give you an overview of the various features and content on the **Request Inquiries** page.

Table 113: Controls in the details pane of a product

Control	Description
Respond	Use this button to respond to the inquiry (see Answering inquiries about requests on page 134).

Table 114: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product.
Request date	Shows when the product was requested.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows you the request number of the total request with which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Auditing (page description)

To open the **Auditing** page go to **Request** > **Auditing**.

On the **Auditing** page, you can:

- Display all requests in the system (see Displaying all requests on page 135)
- Display all approvals in the system (see Displaying all approvals on page 136)

To do this, click on one of the tiles:

Table 115: Tiles

Tiles	Description
Request	Here you can see all the requests. You can also filter them so that only products requested for a specific identity are displayed (see Displaying all requests on page 135).
Approval	Here you can see all the approvals. You can also filter them so that only requests relating to a specific identity are displayed (see Displaying all approvals on page 136).

Auditing – Requests (page description)

To open the **Auditing - Requests** page go to **Request** > **Auditing** > **Request**.

On the **Auditing - Requests** page, you can show all requests (see Displaying all requests on page 135).

If you only want to display requests for a specific identity, use the Advanced search. If you only want to display requests for a specific time period, use the filter function in the **Request date** column.

The following tables give you an overview of the various features and content on the **Auditing – Requests** page.

Table 116: Controls

Control	Description

Advanced search	The advanced search allows you to control which product requests are displayed:
	• **Select identity**: Click **Assign** and select the identity whose requests you want to display. You can then use the following options to control which product requests are displayed:
	  • **Requests submitted by the selected identity for itself**: Select this check box to display product requests placed by the selected identity for themselves.
	  • **Requests submitted by the selected identity for others**: Select this check box to display product requests placed by the selected identity for other identities.
	  • **Requests submitted by others for the selected identity**: Select this check box to display product

Control	Description
	requests placed by other identities for the selected identity. • **Submitted requests in the selected identity's organization**: Select this check box to display product requests placed in the selected identity's scope of responsibility. • **Filter by request number**: Enter the request number of the request you want to display. • **Pending**: Select this check box to display product requests that are not yet approved (status: **Request**). • **Approved**: Select this check box to display product requests that have been granted approval (status: **Assigned**). • **Canceled or denied or unsubscribed**: Select this check box to display product requests that have been canceled, denied, or unsubscribed. Click **Search** to apply the filter criteria. Click **Reset** to reset the filter criteria to the default search.

Table 117: Controls in the details pane of a product

Control	Description
Show details	Use this button to show the details of the entire request used to request this product.

Table 118: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product. The following status' are possible: • **Assigned**: The product request was successful and the product was successfully assigned. • **Request**: The product request is still awaiting an approval decision (it is still in the request workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The product request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The product request was granted approval by the approver and continues along the workflow. In the details pane, on

Column	Description
	the **Workflow** tab, you can see the current position in the workflow. • **Renewal**: The product has been renewed (see Renewing products with limit validity periods on page 130). • **Unsubscription**: The product is being unsubscribed (see Unsubscribing products on page 131). • **Denied**: The request for this product was denied. The reason for denying may be a policy or rule violation or the manager not verifying the request if it is only temporary. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. . • **Canceled**: The product request was canceled or the system could not carry out the request (for example, because an identity for verifying it was not given or the validity period expired). In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed**: The product was unsubscribed (see Unsubscribing products on page 131). In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested. TIP: If you only want to display products that were requested within a certain time period, click (**Filtering: Request date**) next to the column header and select the appropriate options.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows you the request number of the total request with which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Auditing - Approvals (page description)

To open the **Auditing - Approvals** page go to **Request** > **Auditing** > **Approval**.

On the **Auditing - Approvals** page, you can show all the request approvals (see Displaying all approvals on page 136).

If you only want to display approvals for a specific identity, use the Advanced search. If you only want to display requests for a specific time period, use the filter function in the **Request date** column.

The following tables give you an overview of the various features and content on the **Auditing – Approvals** page.

Table 119: Controls

Control	Description
Advanced search	The advanced search allows you to control which approvals are displayed: • **Select approver**: Click **Assign** and select the identity whose approvals you want to display. • **Filter by request number**: Enter the request number of the request you want to display. TIP: To find out the request number of a request, open the request history (see Displaying request history on page 128) and take the request number from the **Shopping Cart** column in the row of the corresponding product. • **Pending**: Select this check box to display product requests that are not yet approved (status: **Request**). • **Approved**: Select this check box to display product requests that have been granted approval (status: **Assigned**). • **Canceled or denied or unsubscribed**: Select this check box to display product requests that have been canceled, denied, or unsubscribed (state: **Canceled**, **Denied**, **Unsubscribed**). Click **Search** to apply the filter criteria to the request history. Click **Reset** to reset the filter criteria to the default search.

Table 120: Controls in the details pane of a product

Control	Description
Show details	Use this button to show the details of the entire request used to request this product.

Table 121: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product.

Column	Description
	The following status' are possible: • **Assigned** – The product request was successful and the product was successfully assigned. • **Request** – The product request is still awaiting an approval decision (it is still in the request workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending** – The product request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved** – The product request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Renewal** – The product has been renewed (see Renewing products with limit validity periods on page 130). • **Unsubscription** – The product is being unsubscribed (see Unsubscribing products on page 131). • **Denied** – The request for this product was denied. The reason for denying may be a policy or rule violation or the manager not verifying the request if it is only temporary. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. . • **Canceled** – The product request was canceled or the system could not carry out the request (for example, because an identity for verifying it was not given or the validity period expired). In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed** – The product was unsubscribed (see Unsubscribing products on page 131). In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows you the request number of the total request with which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

IT Shop escalation (page description)

NOTE: You only see the **IT Shop escalation** page if you are a fallback approver or member of the chief approval team.

Open the **IT Shop Escalation Approval** page by navigating through **Request** > **Escalation**.

If the are requests pending and the approver responsible is not available for an extended period or has no access to Web Portal, then the fallback approver or member of the chief approval team must make an approval decision. For more detailed information about the chief approval team, see the *One Identity Manager IT Shop Administration Guide*.

On the **IT Shop Escalation Approvals** page, you can:

- Display all escalated requests that you can approve (see Displaying escalated requests on page 137)
- Grant or deny requests (see Approving and denying escalated requests on page 138)
- Make inquiries about requests if the information is insufficient to make an approval decision (see Submitting inquiries about escalated requests on page 150)
- Add other approvers that can approve requests (see Appointing additional approvers to escalated requests on page 146)
- Reroute request approvals to other identities (see Rerouting escalated requests' approvals on page 145)
- Delegate request approvals to other identities (see Delegating approvals of escalated requests to other identities on page 147)
- Change the priority of requests (see Changing priority of pending requests on page 123)
- Add more products to existing requests (see Adding more products to escalated requests on page 149)
- Cancel requests (see Canceling escalated requests on page 150)
- Revoke requests' hold status (see Revoking hold status of escalated requests on page 152)

NOTE: To show requests, you must enter at least one filter option.

The following tables give you an overview of the different functions and content on the **Devices** page.IT Shop

Table 122: Controls

Control	Description
Approve	Use this button to approve the product request (see Approving and denying escalated requests on page 138).
Deny	Use this button to deny the product request (see Approving and denying escalated requests on page 138).
Approve all	Use this button to approve the all the product requests shown (see Approving and denying escalated requests on page 138).
Deny all	Use this button to deny the all the product requests shown (see Approving and denying escalated requests on page 138).
Next	Opens the **IT Shop escalation – Approvals** (see IT Shop escalation - Approvals (page description) on page 894). Use this button to show an overview of all approvals made that you still make adjustments to and then save. As long as you have not made an approval decision (by using the appropriate button), this button is disabled.

Table 123: Controls in the details pane of a product

Control	Description
Withdraw request	Use this button to approve the product request (see Canceling escalated requests on page 150).
Revoking hold status	Use this button to release the request for approval again so that it can be processed by the approvers (see Revoking hold status of escalated requests on page 152).
Withdrawing additional approval	If you have appointed an additional approver for this product request (see Appointing additional approvers to escalated requests on page 146), use this button to revoke the action. Then you are the only approver of this product request (see Removing additional approvers from escalated requests on page 147).
Recall last question	Use this button to recall the question that you asked another identity about the product request (see Submitting inquiries about escalated requests on page 150).
Display the identity's entitlements	Use this button to specify which modifications to make to the effective date of change (see Approving new manager's escalated assignments on page 144).
more > Send inquiry	Use this function to send an inquiry to an identity about the product request (see Submitting inquiries about escalated requests on page 150).
more > Show entire request	Use this action to show the entire request that was used to request this product (see Displaying and approving entire requests of

Control	Description
	escalated requests on page 140).
more > Reroute approval	Use this action to let another approval level make the approval decision about a product. For example, if approval is required by a manager in a one-off case (see Rerouting escalated requests' approvals on page 145).
more > Add approver	Use this action to add an additional approver to share the approval decision about the request (see Appointing additional approvers to escalated requests on page 146). You can revoke this action in the approval history (see Removing additional approvers from escalated requests on page 147).
more > Delegate approval	Use this action to delegate the approval decision about the request to another identity (see Delegating approvals of escalated requests to other identities on page 147).
more > Change priority	Use this action to change the priority of the product request (see Changing priority of escalated requests on page 148).

Table 124: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product.
Request date	Shows when the product was requested.
Recipient	Shows for whom the product was requested.
Priority	Shows the priority for this product request.
Approval	Use these two buttons to make an approval decision about the product request. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.

Requests overview (page description)

To open the **Request overview** page go to **Request** > **Escalation** > Details pane > **more** > **Show entire request**.

The **Request overview** page provides an overview of all the products from a specific request and you can approve all the pending product requests (see Displaying and approving entire requests of escalated requests on page 140).

The following tables give you an overview of the different functions and content on the **Request overview** page.

Table 125: Controls

Control	Description
Add items to this request	Opens the **Request** page (see Request (page description) on page 858). Use this button to add more products to the corresponding request (see Adding more products to escalated requests on page 149).
Approve all	Opens the **IT Shop escalation – Approvals** (see IT Shop escalation - Approvals (page description) on page 894). Use this button to approve all pending product requests in this request Displaying and approving entire requests of pending requests on page 113).

Table 126: Controls in the details pane of a product

Control	Description
Cancel	Use this button to cancel the product request (see Canceling escalated requests on page 150).

Table 127: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product. The following status' are possible: • **Assigned**: The request was successful and the product was successfully assigned. • **Request**: The request is still awaiting an approval decision (it is still in the workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The request is waiting for an approval decision from an

Column	Description
	approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Renew**: The product was just renewed. • **Unsubscription**: The product is being unsubscribed. • **Deny**: The request was denied. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. • **Canceled**: The request was canceled. In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed**: The request was unsubscribed. In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows the request shopping cart from which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

IT Shop escalation - Approvals (page description)

To open the **IT Shop escalation – Approvals** page go to **Request** > **Escalation** > Make approval decision > **Next**.

After you have made your approval decisions on the **IT Shop Escalation Approvals** page, you can save the approval on the **IT Shop Escalation – Approvals** page so that they take effect (see Approving and denying escalated requests on page 138). You can also enter reason for the approval decisions here.

The following tables give you an overview of the different functions and content on the **IT Shop Escalation – Approvals** page.

Table 128: Controls

Control	Description
Reason for approvals	Here you can enter a reason for all approved product requests.
Standard reason	Here you can select one of the standard reasons saved in the system for all approved product requests.
Reason for denials	Here you can enter a reason for all denied product requests.
Standard reason	Here you can select one of the standard reasons saved in the system for all denied product requests.
Save	Use this button to save all the settings and approval decisions.
Back	Use this button to switch to the previous page. For example, to approve other product requests.

Table 129: Columns

Column	Description
Product	Shows the name of the product that was requested.
Recipient	Shows for whom the product was requested.
Valid from	Here you can specify from when the product is valid (see Changing priority of escalated requests on page 148).
Valid until	Here you can specify until when the product is valid (see Changing priority of escalated requests on page 148).
Reason	Here you can enter a reason for the decision. To do this, click on the link and, in the dialog, enter a reason or select one of the standard reasons.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation (Menu description)

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to

describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

You can use items on the **Attestation** menu to perform various actions and collect information. The following tables provide you with an overview of the menu items and actions that can be run here.

Table 130: Menu items

Menu	Menu item		Description
Attestation			
	My attestation status		You can select the following actions: • Display attestation cases that affect you (see Displaying your attestation cases on page 175) • Display attestors for pending attestation cases (see Displaying attestors of my attestation cases on page 163) • Send reminders to approvers (see Sending reminders for your own attestation cases on page 168)
	My actions		
		Pending attestations	Make approval decisions about pending attestations.
		Attestation history	View all the approvals that you made about attestations.
		Attestation inquiries	Display and answer attestation inquiries submitted within the scope of an approval workflow.
	Auditing		Display all attestations.
	Governance administration		

Menu	Menu item		Description
		Attestation runs	Display an attestation prediction and an overview of pending attestation cases.
		Attestation policy settings	Display or create attestation policies.
	Escalation		Make decisions about escalating attestations.

My attestation status (page description)

To open the **My Attestation Status** page go to **Attestation** > **My Attestation Status**.

On the **Attestation Status** page, you can:

- Display attestation cases that affect you (see Displaying your attestation cases on page 175)
- Display attestors for pending attestation cases (see Displaying attestors of my attestation cases on page 163)
- Send reminders to approvers (see Sending reminders for your own attestation cases on page 168)

The attestation cases are divided into different sections on the following tabs to provide a clearer overview:

- **Memberships**: Shows you all attestation cases that relate to memberships in objects.
- **User accounts**: Shows you all attestation cases that relate to user accounts.
- **Group memberships**: Shows all the attestation cases that relate to memberships in groups.
- **Object** attestation: Shows you all attestation cases that relate to the attestation of specific objects.
- **All attestation cases**: Shows all the attestation cases.

The following tables give you an overview of the various features and content on the **My Attestation Status** page.

Table 131: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my attestation cases on page 163) and send them reminder mails (see Sending reminders for your own attestation cases on page 168).

Control	Description
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders for your own attestation cases on page 168).
Approve	Opens the **Pending Attestations – Identity** page (see Pending attestations – Identity (page description) on page 932). Use this button to gran or deny approval to pending attestation cases that affect you (see Granting or denying my attestation cases on page 176).

Table 132: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my attestation cases on page 163). Then you can send them reminder mails (see Sending reminders for your own attestation cases on page 168).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying your attestation cases on page 175).

Table 133: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Denied**: The attestation case has been denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

My actions (page description)

To open the **My Actions** page go to **Attestation** > **My Actions**.

On the **My Actions** page, you can perform various actions for attestation cases in which you are involved as an approver.

To do this, click on one of the tiles:

Table 134: Tiles

Tiles	Description
Pending attestations	You select the following actions: • Display pending attestation cases (see Displaying pending attestation cases on page 178) • Make approval decisions about attestation cases (see Pending attestations on page 177)
Attestation history	You can display all approvals of attestation cases that you, or the identities that report to you, decided upon.
Attestation inquiries	Here you can perform the following actions in response to questions you have been asked about specific attestation cases: • Show inquiries (see Displaying attestation case inquiries on page 189) • Answer inquiries (see Answering attestation case inquiries on page 190)

Pending attestations (page description)

To open the **Pending Attestations** page go to **Attestation** > **My Actions** > **Pending Attestations**.

On the **Pending Attestations** page, you can select object types for which pending attestation cases exist and then approve or deny them.

Use the **Switch to policy view** button to display all existing attestation cases grouped by the associated attestation policy and then make your approval decisions about the attestation cases (see Pending attestations – Attestation policies (page description) on page 900).

To make it easier to follow, the objects to be attested are grouped and accessible over tiles. Click one of the following tiles and then select the object to be attested:

- One Identity Manager application roles
- Departments
- System roles
- Locations
- Business roles
- PAM assets
- PAM user accounts
- Identities
- Cost centers
- User accounts
- System entitlements
- Devices

Pending attestations – Attestation policies (page description)

To open the **Pending Attestations - Attestation Policies** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Switch to policy view**.

On the **Pending Attestations - Attestation Policies** page, you can display all existing attestation cases grouped by the corresponding attestation policy. If you click on an entry in the list, you can then approve the corresponding attestation cases (see Granting or denying attestation cases on page 179).

The following table gives you an overview of the different controls on the **Pending Attestations – Attestation policies** page.

Table 135: Columns

Column	Description
Attestation policy	Shows you the name of the attestation policy for which there are pending attestation cases.
Attestation Cases	Shows you how many pending attestation cases there are for this attest-ation policy and whether they are overdue.

Column	Description
Review	Shows you how many attestation cases of the current attestation runs have already been approved.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Attestation policy (page description) role

To open the **Pending Attestations – Attestation Policy** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Switch to policy view** > select an attestation policy.

On the **Pending Attestations – Attestation Policy** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – attestation policy** page.

Table 136: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 137: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate	Use this action to delegate the approval decision about the attestation

Control	Description
approval	case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 138: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on

Column	Description
	the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: One Identity Manager application roles (page description)

To open the **Pending Attestations: One Identity Manager application roles** page go to **Attestation** > **My Actions** > **Pending Attestations** > **One Identity Manager application roles**.

On the **Pending Attestations: One Identity Manager application roles** page, you can see all the application roles with pending attestation cases that you can approve. If you click on an application role, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Application role (page description) on page 905).

The following table gives you an overview of the different controls on the **Pending Attestations: One Identity Manager application roles** page.

Table 139: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Application role (page description)

To open the **Pending Attestations – Application role** page go to **Attestation** > **My Actions** > **Pending Attestations** > **One Identity Manager application roles** > select application role.

On the **Pending Attestations – Application role** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Application role** page.

Table 140: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 141: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate	Use this action to delegate the approval decision about the attestation

Control	Description
approval	case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 142: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on

Column	Description
	the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Departments (page description)

To open the **Pending Attestations: Departments** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Departments**.

On the **Pending Attestations: Departments** page, you can see all the departments with pending attestation cases that you can approve. If you click on a department, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Department (page description) on page 909).

The following table gives you an overview of the different controls on the **Pending Attestations: Departments** page.

Table 143: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view.

Control	Description
	TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Department (page description)

To open the **Pending Attestations – Department** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Departments** > select a department.

On the **Pending Attestations – Department** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Department** page.

Table 144: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).

Control	Description
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 145: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 146: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.

Column	Description
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: System roles (page description)

To open the **Pending Attestations: System roles** page go to **Attestation** > **My Actions** > **Pending Attestations** > **System roles**.

On the **Pending Attestations: System roles** page, you can see all the system roles with pending attestation cases that you can approve. If you click on a system role, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – System role (page description) on page 912).

The following table gives you an overview of the different controls on the **Pending Attestations: System roles** page.

Table 147: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – System role (page description)

To open the **Pending Attestations – System role** page go to **Attestation** > **My Actions** > **Pending Attestations** > **System roles** > select a system role.

On the **Pending Attestations – System role** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – System role** page.

Table 148: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that

Control	Description
	still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 149: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional

Control	Description
	approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 150: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Locations (page description)

To open the **Pending Attestations: Locations** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Locations** .

On the **Pending Attestations: Locations** page, you can see all the locations with pending attestation cases that you can approve. If you click on a location, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Location (page description) on page 916).

The following table gives you an overview of the different controls on the **Pending Attestations: Locations** page.

Table 151: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Location (page description)

To open the **Pending attestations – Location** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Locations** > select a location.

On the **Pending Attestations – Location** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest

- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Location** page.

Table 152: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 153: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 154: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Business roles (page description)

To open the **Pending Attestations: Business roles** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Business roles**.

On the **Pending Attestations: Business Roles** page, you can see all the business roles with pending attestation cases that you can approve. If you click on a business role, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Business role (page description) on page 920).

The following table gives you an overview of the different controls on the **Pending Attestations: Business roles** page.

Table 155: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Business role (page description)

To open the **Pending Attestations – Business role** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Business roles** > select a business role.

On the **Pending Attestations – Business role** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)

- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Business role** page.

Table 156: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 157: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).

Control	Description
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 158: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.

Column	Description
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: PAM assets (page description)

To open the **Pending Attestations: PAM assets** page go to **Attestation** > **My Actions** > **Pending Attestations** > **PAM assets**.

On the **Pending Attestations: PAM assets** page, you can see all the PAM assets with pending attestation cases that you can approve. If you click on a PAM asset, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – PAM asset (page description) on page 924).

The following table gives you an overview of the different controls on the **Pending Attestations: PAM assets** page.

Table 159: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – PAM asset (page description)

To open the **Pending Attestations – PAM asset** page go to **Attestation** > **My Actions** > **Pending Attestations** > **PAM assets** > select a PAM asset.

On the **Pending Attestations – PAM user account** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – PAM asset** page.

Table 160: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 161: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate	Use this action to delegate the approval decision about the attestation

Control	Description
approval	case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 162: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on

Column	Description
	the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: PAM user accounts (page description)

To open the **Pending Attestations: PAM user accounts** page go to **Attestation** > **My Actions** > **Pending Attestations** > **PAM user accounts**.

On the **Pending Attestations: PAM user accounts** page, you can see all the PAM user accounts with pending attestation cases that you can approve. If you click on a PAM user account, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – PAM user account (page description) on page 928).

The following table gives you an overview of the different controls on the **Pending Attestations: PAM user accounts** page.

Table 163: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – PAM user account (page description)

To open the **Pending Attestations – PAM user account** page go to **Attestation** > **My Actions** > **Pending Attestations** > **PAM user accounts** > select a PAM user account.

On the **Pending Attestations – PAM user account** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – PAM user account** page.

Table 164: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 165: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate	Use this action to delegate the approval decision about the attestation

Control	Description
approval	case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 166: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on

Column	Description
	the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Employees (page description)

To open the **Pending Attestations: Employees** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Employees**.

On the **Pending Attestations: Employees** page, you can see all the identities with pending attestation cases that you can approve. If you click on an identity, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Identity (page description) on page 932).

The following table gives you an overview of the different controls on the **Pending Attestations: Employees** page.

Table 167: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view.

Control	Description
	TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Identity (page description)

To open the **Pending attestations – Identity** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Employees** > Select an identity.

On the **Pending Attestations – Identity** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Identity** page.

Table 168: Controls

Control	Description
☑ Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
☒ Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).

Control	Description
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 169: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 170: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.

Column	Description
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Cost centers (page description)

To open the **Pending Attestations: Cost centers** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Cost centers**.

On the **Pending Attestations: Cost centers** page, you can see all the cost centers with pending attestation cases that you can approve. If you click on a cost centers, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Cost center (page description) on page 935).

The following table gives you an overview of the different controls on the **Pending Attestations: Cost centers** page.

Table 171: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Cost center (page description)

To open the **Pending Attestations – Cost center** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Cost centers** > select a cost center.

On the **Pending Attestations – Cost center** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Cost center** page.

Table 172: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that

Control	Description
	still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 173: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional

Control	Description
	approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 174: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: User accounts (page description)

To open the **Pending Attestations: User accounts** page go to **Attestation** > **My Actions** > **Pending Attestations** > **User accounts**.

On the **Pending Attestations: User accounts** page, you can see all the user accounts with pending attestation cases that you can approve. If you click on a user account, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – User account (page description) on page 939).

The following table gives you an overview of the different controls on the **Pending Attestations: User accounts** page.

Table 175: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – User account (page description)

To open the **Pending Attestations – User account** page go to **Attestation** > **My Actions** > **Pending Attestations** > **User accounts** > select a user account.

On the **Pending Attestations – User account** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest

- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – user account** page.

Table 176: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 177: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 178: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: System entitlements (page description)

To open the **Pending Attestations: System entitlements** page go to **Attestation** > **My Actions** > **Pending Attestations** > **System entitlements**.

On the **Pending Attestations: System entitlements** page, you can see all the system entitlements with pending attestation cases that you can approve. If you click on a system entitlement, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – System entitlement (page description) on page 943).

The following table gives an overview of the different controls on the **Pending Attestations: System entitlements** page.

Table 179: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – System entitlement (page description)

To open the **Pending Attestations – System entitlement** page go to **Attestation** > **My Actions** > **Pending Attestations** > **System entitlements** > select a system entitlement.

On the **Pending Attestations – System entitlement** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)

- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – System entitlement** page.

Table 180: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 181: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).

Control	Description
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 182: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.

Column	Description
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Resources (page description)

To open the **Pending Attestations: Resources** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Resources**.

On the **Pending Attestations: Resources** page, you can see all the resources with pending attestation cases that you can approve. If you click on a resource, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Resource (page description) on page 947).

The following table gives you an overview of the different controls on the **Pending Attestations: Resources** page.

Table 183: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Resource (page description)

To open the **Pending attestations – Resource** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Resources** > Select a resource.

On the **Pending Attestations – Resource** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Resource** page.

Table 184: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 185: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate	Use this action to delegate the approval decision about the attestation

Control	Description
approval	case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 186: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on

Column	Description
	the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Assignment resources (page description)

To open the **Pending Attestations: Assignment resources** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Assignment resources**.

On the **Pending Attestations: Assignment resources** page, you can see all the assignment resources with pending attestation cases that you can approve. If you click on an assignment resource, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Assignment resource (page description) on page 951).

The following table gives you an overview of the different controls on the **Pending Attestations: Assignment resources** page.

Table 187: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Assignment resource (page description)

To open the **Pending attestations – Assignment resource** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Assignment resources** > Select an assignment resource.

On the **Pending Attestations – Assignment resource** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Assignment resource** page.

Table 188: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 189: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate	Use this action to delegate the approval decision about the attestation

Control	Description
approval	case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 190: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on

Column	Description
	the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestation: Multi-request resources (page description)

To open the **Pending Attestations: Multi-request resources** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Multi-request resources**.

On the **Pending Attestations: Multi-request resources** page, you can see all the multi-request resources with pending attestation cases that you can approve. If you click on a multi-request resource, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestation – Multi-request resource (page description) on page 955).

The following table gives you an overview of the different controls on the **Pending Attestations: Multi-request resources** page.

Table 191: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestation – Multi-request resource (page description)

To open the **Pending attestations – Multi-request resource** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Multi-request resources** > Select a multi-request resource.

On the **Pending Attestations – Multi-request resource** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Multi-request resource** page.

Table 192: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 193: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate	Use this action to delegate the approval decision about the attestation

Control	Description
approval	case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 194: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on

Column	Description
	the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Software (page description)

To open the **Pending Attestations: Software** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Software**.

On the **Pending Attestations: Software** page, you can see all the software applications with pending attestation cases that you can approve. If you click on a software application, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Software (page description) on page 959).

The following table gives you an overview of the different controls on the **Pending Attestations: Software** page.

Table 195: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view.

Control	Description
	TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Software (page description)

To open the **Pending attestations – Software** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Software** > Select a software application.

On the **Pending Attestations – Software** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Software** page.

Table 196: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).

Control	Description
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 197: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 198: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.

Column	Description
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Multi requestable/unsubscribable resources (page description)

To open the **Pending Attestations: Multi requestable/unsubscribable resources** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Multi requestable/unsubscribable resources**.

On the **Pending Attestations: Multi requestable/unsubscribable resources** page, you can see all the multi requestable/unsubscribable resources with pending attestation cases that you can approve. If you click on a multi requestable/unsubscribable resource, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations – Multi requestable/unsubscribable resource (page description) on page 963).

The following table gives you an overview of the different controls on the **Pending Attestations: Multi requestable/unsubscribable resources** page.

Table 199: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations – Multi requestable/unsubscribable resource (page description)

To open the **Pending attestations – Multi requestable/unsubscribable resource** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Multi requestable/unsubscribable resources** > Select a multi requestable/unsubscribable resource.

On the **Pending Attestations – Multi requestable/unsubscribable resource** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Multi requestable/unsubscribable resource** page.

Table 200: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).

Control	Description
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 201: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 202: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.

Column	Description
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations: Devices (page description)

To open the **Pending Attestations: Devices** page go to **Attestation** > **My Actions** > **Pending Attestations** > **Devices**.

On the **Pending Attestations: Devices** page, you can see all the devices with pending attestation cases that you can approve. If you click on a device, a new page opens where you can make approval decisions about the attestation cases and run other tasks (see Pending attestations: Device (page description) on page 966).

The following table gives you an overview of the different controls on the **Pending Attestations: Devices** page.

Table 203: Controls

Control	Description
Tree view	Use this button to switch to the tree/hierarchical view.
List view	Use this button to switch to the detailed list view. TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Pending attestations: Device (page description)

Open the **Pending Attestations – Device** page by navigating through **Attestation** > **My Actions** > **Pending Attestations** > **Devices** > Select device.

On the **Pending Attestations – Device** page, you can:

- Display pending attestation cases (see Displaying pending attestation cases on page 178)
- Display attestors for pending attestation cases (see Displaying attestors of pending attestation cases on page 164)
- Display object details to attest (see Displaying pending attestation cases on page 178)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about pending attestation cases on page 169)
- Grant or deny attestation cases (see Granting or denying attestation cases on page 179)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about pending attestation cases on page 185)
- Reroute attestation case approvals to other identities (see Rerouting approvals of pending attestation cases on page 181)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to pending attestation cases on page 182)
- Delegate attestation case approvals to other identities (see Delegating approvals of pending attestation cases to other identities on page 183)
- Revoke attestation cases' hold status (see Revoking the hold status of pending attestation cases on page 187)

The following tables give you an overview of the various features and content on the **Pending Attestations – Device** page.

Table 204: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying attestation cases on page 179).
Deny	Use this button to deny the attestation approval (see Granting or denying attestation cases on page 179).
Approve all	Use this button to grant all attestations approval (see Granting or denying attestation cases on page 179).
Deny all	Use this button to deny all attestations approval (see Granting or denying attestation cases on page 179).
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases on page 164) and send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Send reminder	You can use this button to send reminder mails to all identities that

Control	Description
	still have attestation cases to approve on the current tab (see Sending reminders about pending attestation cases on page 169).
Next	Opens the **Pending Attestations – Approvals** (see Pending attestations – approvals (page description) on page 970). Use this button to display an overview of all approvals made and set further options (see Granting or denying attestation cases on page 179). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 205: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying pending attestation cases on page 178).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about pending attestation cases on page 185).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of pending attestation cases on page 181).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to pending attestation cases on page 182).
Actions > Delegate approval	Use this action to delegate the approval decision about the attestation case to another identity (see Delegating approvals of pending attestation cases to other identities on page 183). You can revoke this action in the attestation history (see Withdrawing delegations from pending attestation case approvals on page 184).
Actions > Reject approval	Use this action to reject the approval decision about an attestation case (see Rejecting approval of attestation cases on page 184). The approval decision is returned to the original approver.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases on page 164). send them reminder mails (see Sending reminders about pending attestation cases on page 169).
Withdrawing additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to pending attestation cases on page 182), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional

Control	Description
	approvers from pending attestation cases on page 182).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of pending attestation cases on page 187).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying pending attestation cases on page 178).

Table 206: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Pending attestations – approvals (page description)

To open the **Pending Attestations – Approvals** page go to **Attestation** > **My Actions** > **Pending Attestations** > Make decision > **Next**.

After you have made your approval decisions on the **Pending Attestations** page, you can save the approval decisions on the **Pending Attestations – Approvals** page so that they take effect. You can also enter reason for the approval decisions here.

The following tables give you an overview of the various features and content on the **Pending Attestations – Approvals** page.

Table 207: Controls

Control	Description
Reason for approvals	Enter a reason for all approved attestations here.
Standard reason	Here you can select one of the standard reasons saved in the system for all approved attestations.
Reason for denials	Enter a reason for all denied attestations here.
Standard reason	Here you can select one of the standard reasons saved in the system for all denied attestations.
Save	Use this button to save all the settings and approval decisions.
Back	Use this button to switch to the previous page. For example, to approve other attestations.

Table 208: Columns

Column	Description
Display name	Shows you the name of the object to be attested.
Attestation	Shows the name of the attestation policy in use.

Column	Description
policy	
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Reason	Here you can enter a reason for the decision. To do this, click on the button and, in the dialog, enter a reason or select one of the standard reasons.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation history (page description)

To open the **Attestation History** page go to **Attestation** > **My actions** > **Attestation History**.

On the **Attestation History** page, you can display all the attestation approval decisions that you or identities for which you are responsible have made (see Displaying attestation history on page 188).

The following tables give you an overview of the various features and content on the **Attestation History** page.

Table 209: Controls

Control	Description
Attestation Status	The check boxes allow you to control which approvals are displayed: • **Approved**: Select this check box to display attestation cases that have been granted approval. • **Pending**: Select this check box to display attestation cases that you have made an approval decision about but have not yet been approved. • **Not approved**: Select this check box to display attestation cases that have been denied.
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending attestation cases through the attestation history on page 165) and send them reminder mails.

Table 210: Controls in the attestation case's details pane

Control	Description
Actions > Go to	Use this action to switch to an overview of the object to be attested

Control	Description
attested object	(see Displaying attestation history on page 188).
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending attestation cases through the attestation history on page 165). Then you can send them reminder mails.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying attestation history on page 188).
Report	Use this button to generate a report about the object to attest.

Table 211: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Approved**: The attestation case was approved. • **Pending**: The attestation case is not closed yet and must still be approved. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.

- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Attestation inquiries (page description)

To open the **Attestation Inquiries** page go to **Attestation** > **My actions** > **Attestation Inquiries**.

On the **Attestation Inquiries** page, you can perform the following actions in response to questions you have been asked about specific attestation cases:

- Show inquiries (see Displaying attestation case inquiries on page 189)
- Answer inquiries (see Answering attestation case inquiries on page 190)

The following tables give you an overview of the various features and content on the **Attestation Inquiries** page.

Table 212: Controls in the attestation case's details pane

Control	Description
Respond	Use this button to respond to the inquiry (see Answering attestation case inquiries on page 190).

Table 213: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.

- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Auditing (page description)

To open the **Auditing** page go to **Attestation** > **Auditing**.

On the **Auditing** page, you can display all the attestation cases in the system.

The following tables give you an overview of the various features and content on the **Auditing** page.

Table 214: Controls

Control	Description
Attestors	Click **Assign** and select the identity whose attestation cases you want to display.
Attestation state	The check boxes allow you to control which approvals are displayed: • **Approved**: Select this check box to display attestation cases that have been granted approval. • **Pending**: Select this check box to display attestation cases that have not yet been approved. • **Not approved**: Select this check box to display attestation cases that have been denied.
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of pending auditing attestation cases on page 166) and send them reminder mails.

Table 215: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested.
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of pending auditing attestation cases on page 166). send them reminder mails.
Viewing details	Use this button to show the details of the entire request used to request this product.
Report	Use this button to generate a report about the object to attest.

Table 216: Columns

Column	Description
Display name	Shows you the name of the object included in the attestation case.
Attestation policy	Shows you the name of the attestation policy in use.
State	Shows you the current status of the attestation case. The following status' are possible: • **Approved**: The attestation case was approved. • **Pending**: The attestation case is not closed yet and must still be approved. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows you whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows you by when the attestation case must be completed.
Risk index	Shows you the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Governance administration (page description)

Open **Governance Administration** page go to **Attestation** > **Governance Administration**.

Attestations start with attestation policies. You use these policies to specify which objects are designated for attestation and when and how often they are run.

Managers or others responsible for compliance can use attestation policies to run the following tasks.

- Authorize access
- Setting up permissions

On the **Governance Administration** page you can perform various actions to do with attestation policies and attestation runs.

To do this, click on one of the tiles:

Table 217: Tiles

Tiles	Description
Attestation runs	You select the following actions: • Display attestations runs whose progress is shown as a prediction • Renew attestation runs • Send approver reminders
Attestation policy settings	You select the following actions: • Displaying attestation policies • Setting up attestation policies • Copying attestation policies • Editing attestation policies • Deleting attestation policies

Attestation runs (page description)

To open the **Attestation runs** page go to **Attestation** > **Governance Administration** > **Attestation runs.**

On the **Attestation Runs** page, you can:

- Display attestations runs whose progress is shown as a prediction
- Renew attestation runs
- Send approver reminders

The following tables give you an overview of the different functions and content on the **Attestation runs** page.

Table 218: Controls

Control	Description
Min Category	You can use the options to select the attestation runs you want to display:

Control	Description
	• **Good**: Displays attestation runs that are rated as good. • **Mediocre**: Displays attestation runs that are rated as mediocre. • **Bad**: Displays attestation runs that are rated as bad.
Reminder attestors of all visible runs	Use this button to send reminder emails to all identities that still have attestation cases to approve in the attestation runs displayed.

Table 219: Controls in the attestation policy's details pane

Control	Description
Extending an attestation run	Use this button to renew the attestation run.
Send reminder	Use this button to send reminder emails to all identities that still have attestation cases to approve in the selected attestation runs.
Attestors > Send reminder	Use this button to send reminder emails to individual identities that still have attestation cases to approve in the selected attestation runs.

Table 220: Columns

Column	Description
Attestation policy	Shows the name of the attestation policy used in the attestation run.
Run started	Show when the attestation run started.
Due date	Shows when the attestation case must be completed.
Progress so far	Show the progress of completed attestation cases in this attestation run. The color of the bar refers to the percentage of the attestation run's progress. • Red: Progress under 70% • Orange: Progress between 70% and 90% • Green: Progress over 90%

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: On the following tabs, you can show other useful information about each attestation run in the pane. To do this, click the appropriate instance in the list.

- **Details**: Shows general information about attestation runs, details of associated attestation cases and an attestation prediction.

- **Attestors**: Show the attestors for the selected attestation runs along with the number of pending and closed attestation cases. You can select attestors and send a reminder email.

Managing attestation policy (page description)

To open the **Attestation Policy Settings** page go to **Attestation** > **Governance Administration** > **Attestation Policy Settings**.

On the **Attestation Policy Settings** page, you can:

- Display attestation policies
- Set up attestation policies
- Copy attestation policies
- Edit attestation policies
- Delete attestation policies

The following tables give you an overview of the various features and content on the **Attestation Policy Settings** page.

Table 221: Controls

Control	Description
Edit	Opens the **Edit attestation policy** page (see Editing attestation policies (page description) on page 982). Use this button to edit the attestation policy. For example, you can: • Set up a schedule after the attestation case is generated • Disable the attestation policy • Select an identity to be responsible for granting or denying approval of attestation cases • Enable or disable automatic closing of obsolete attestation cases by the system • Create/edit condition for ascertaining which objects to attest
Copy	Use this button to copy the attestation policy.
Delete	Use this button to delete the attestation policy.
Show disabled policies	Use this button to display disabled attestation policies. For example, you can display a disabled attestation policy to edit and re-enable it.
New attestation policy	Use this button to create a new attestation policy. This opens the **Create New Attestation Policy** page.

Table 222: Columns

Column	Description
Attestation policy	Shows you the name of the attestation policy.
Attestation procedure	Shows you the name of the attestation procedure used by the attestation policy.
Compliance frameworks	Shows you the name of the compliance frameworks used by the attestation policy. Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements. This could be internal requirements or auditing requirements.
Calculation schedule	Shows you how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.
Owner	Shows you the name of the identity that created the attestation policy.
Actions	Using the buttons (see the previous table) you can edit, copy, or delete the attestation policy.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Creating new attestation policies (page description)

To open the **Create New Attestation Policy** page go to **Attestation** > **Governance Administration** > **Attestation Policy Settings** > **New attestation policy**.

On the **Create New Attestation Policy** page you can create a new attestation policy.

The following tables give you an overview of the various features and content on the **Attestation Policy Settings** page.

Table 223: Controls

Control	Description
Create	Use this button to save the attestation policy with your settings.
Cancel	Use this button to cancel creation of the new attestation policy.

You can specify the following main data.

Table 224: Attestation policy main data

Property	Description
Disabled	Specify whether the attestation policy is disabled or not. Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Completed attestation cases can be deleted once the attestation policy is disabled.
Attestation policy	Enter a name for the attestation policy.
Description	Enter a description of the attestation policy.
Attestation procedure	Click **Assign**/**Change** and specify which objects will be attested with this attestation policy. NOTE: The selection of the attestation procedure is crucial. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The available options are modified to match the attestation procedure.
Approval policies	Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.
Attestors	Click **Assign**/**Change** and then select the identities that can make approval decisions about attestation cases. NOTE: This field is only shown if you have selected an attestation policy in the **Attestation policy** menu that demands attestation by an approver (for example, **Attestation by selected approvers**).
Calculation schedule	Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.
Time required (days)	Specify how many days attestors have to make an approval decision about the attestation cases governed by this policy. If you do not want to specify a time, enter **0**.
Owner	Select the identity that is responsible for this attestation policy. This identity can view and edit the attestation policy.
Risk index	Use the slider to define the attestation policy's risk index. This value specifies the risk for the company if attestation for this attestation policy is denied.
Compliance frameworks	Click **Assign**/**Change** and add a compliance framework to use. Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements. For example, internal requirements or auditing requirements.

Property	Description
Close obsolete tasks automatically	Specify whether attestation cases pending for this attestation policy are automatically closed if new attestation cases are created (for example, when there is a new attestation run of this attestation policy). If an attestation run with this attestation policy is started and the option is set, new attestation cases are created according to the condition. All pending, obsolete attestation cases for newly determined attestation objects of this attestation policy are stopped. Attestation cases for attestation objects that are not recalculated, remain intact.
Approval by multi-factor authentication	Specify whether approvals about attestation cases governed by this attestation policy require multifactor authentication.

In the **Object selection**, you use conditions to specify which objects are to be attested. The following table gives you an overview of the various features in the **Object selection** view.

Table 225: Controls in the object selection

Control	Description
All conditions must be fulfilled:	Enable this option to have new attestation cases created for all objects that meet each of the conditions the next time the attestation policy is run. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.
At least one condition must be fulfilled:	Enable this option so that new attestation cases are created for all objects that meet at least one of the conditions the next time the attestation policy is run. Use of this option generates a superset of all the individual conditions of the selected objects.
Add condition	Use this button to create a new condition. Conditions specify which objects to attest. For more information about the different conditions, see Appendix: Attestation conditions and approval policies from attestation procedures on page 808.
Number of objects matching in total	Click the displayed number to preview all objects that to attest.
Edit condition	Use this button to edit an existing condition.
Delete condition	Use this button to delete and an existing condition.
Refresh	Use this button to update the total number of matching objects.

Editing attestation policies (page description)

To open the **Edit attestation policy** page go to **Attestation** > **Governance Administration** > **Attestation Policy Settings** > (**Edit attestation policy**).

On the **Edit attestation policy** page, you can:

- Set up a schedule after the attestation case is generated
- Disable the attestation policy
- Select an identity to be responsible for granting or denying approval of attestation cases
- Enable or disable automatic closing of obsolete attestation cases by the system
- Create/edit condition for ascertaining which objects to attest

The following tables give you an overview of the various features and content on the **Edit attestation policy** page.

Table 226: Controls

Control	Description
Save	Use this button to save the attestation policy with the changes you have made.
Delete	Use this button to delete the attestation policy.
Cancel	Use this button to discard the changes to the attestation policy.

You can change the following main data.

Table 227: Attestation policy main data

Property	Description
Disabled	Specify whether the attestation policy is disabled or not. Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Completed attestation cases can be deleted once the attestation policy is disabled.
Attestation policy	Enter a name for the attestation policy.
Description	Enter a description of the attestation policy.
Attestation procedure	Click **Assign/Change** and specify which objects will be attested with this attestation policy. NOTE: The selection of the attestation procedure is crucial. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The available options are modified to match the attestation procedure.

Property	Description
Approval policies	Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.
Attestors	Click **Assign**/**Change** and then select the identities that can make approval decisions about attestation cases. NOTE: This field is only shown if you have selected an attestation policy in the **Attestation policy** menu that demands attestation by an approver (for example, **Attestation by selected approvers**).
Calculation schedule	Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.
Time required (days)	Specify how many days attestors have to make an approval decision about the attestation cases governed by this policy. If you do not want to specify a time, enter **0**.
Owner	Select the identity that is responsible for this attestation policy. This identity can view and edit the attestation policy.
Risk index	Use the slider to define the attestation policy's risk index. This value specifies the risk for the company if attestation for this attestation policy is denied.
Compliance frameworks	Click **Assign**/**Change** and add a compliance framework to use. Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements. For example, internal requirements or auditing requirements.
Close obsolete tasks automatically	Specify whether attestation cases pending for this attestation policy are automatically closed if new attestation cases are created (for example, when there is a new attestation run of this attestation policy). If an attestation run with this attestation policy is started and the option is set, new attestation cases are created according to the condition. All pending, obsolete attestation cases for newly determined attestation objects of this attestation policy are stopped. Attestation cases for attestation objects that are not recalculated, remain intact.
Approval by multi-factor authentication	Specify whether approvals about attestation cases governed by this attestation policy require multifactor authentication.

In the **Object selection**, you use conditions to specify which objects are to be attested. The following table gives you an overview of the various features in the **Object selection** view.

Table 228: Controls in the object selection

Control	Description
Adding conditions	Use this button to create a new condition. Conditions specify which objects to attest. For more information about the different conditions, see Appendix: Attestation conditions and approval policies from attestation procedures on page 808.
Number of objects matching in total	Click the displayed number to preview all objects that to attest.
Editing conditions	Use this button to edit an existing condition.
Deleting conditions	Use this button to delete and an existing condition.
Refresh	Use this button to update the total number of matching objects.

Attestation escalation approval (page description)

To open the **Attestation Escalation Approval** page go to **Attestation** > **Escalation**.

If the are attestations pending and the approver responsible is not available for an extended period or has no access to Web Portal, the fallback approver or member of the chief approval team must make an approval decision. For more information about the chief approval team, see the One Identity Manager Attestation Administration Guide.

On the **Attestation Escalation Approval**, you can display attestation cases grouped by attestation policy and then, on the **Attestation Escalation Approval - <attestation policy>** page, approve the attestation cases (see Attestation escalation approval – Attestation policy (page description) on page 985).

The following table gives you an overview of the various features on the **Attestation Escalation Approval** page.

Table 229: Columns

Column	Description
Attestation policy	Shows you the name of the attestation policy for which there are pending attestation cases.
Attestation Cases	Shows you how many pending attestation cases there are for this attestation policy and whether they are overdue.
Review	Shows you the progress of completed attestation cases in this attestation run. The color of the bar refers to the percentage of the attestation run's

Column	Description
	progress. • Red: Progress under 70% • Orange: Progress between 70% and 90% • Green: Progress over 90%

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation escalation approval – Attestation policy (page description)

To open the **Attestation Escalation Approval – Attestation policy** page go to **Attestation** > **Escalation** > select attestation policy.

On the **Attestation Escalation Approval – Attestation policy** page, you can:

- Display escalated attestation cases (see Displaying escalated attestation cases on page 192)
- Display attestors for escalated attestation cases (see Displaying attestors of escalated attestation cases on page 166)
- Display object details to attest (see Displaying escalated attestation cases on page 192)
- Generate reports about objects to attest
- Send reminders to approvers (see Sending reminders about escalated attestation cases on page 173)
- Grant or deny attestation cases (see Granting or denying escalated attestation cases on page 194)
- Make inquiries about attestation cases if the information is insufficient to make an approval decision (see Submitting inquiries about escalated attestation cases on page 198)
- Reroute attestation case approvals to other identities (see Rerouting approvals of escalated attestation cases on page 195)
- Add other approvers that can approve attestation cases (see Appointing additional approvers to escalated attestation cases on page 196)
- Delegate attestation case approvals to other identities (see Delegating approvals of escalated attestation cases to other identities on page 197)
- Revoke attestation cases' hold status (see Revoking the hold status of escalated attestation cases on page 200)

The following tables give you an overview of the various features and content on the **Attestations Escalation Approval – attestation policy** page.

Table 230: Controls

Control	Description
Approve	Use this button to grant the attestation approval (see Granting or denying escalated attestation cases on page 194).
Deny	Use this button to deny the attestation approval (see Granting or denying escalated attestation cases on page 194).
Approve all	Use this button to grant all attestations approval (see Granting or denying escalated attestation cases on page 194).
Deny all	Use this button to deny all attestations approval (see Granting or denying escalated attestation cases on page 194).
View attestors for pending attestation cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of escalated attestation cases on page 166) and send them reminder mails (see Sending reminders about escalated attestation cases on page 173).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about escalated attestation cases on page 173).
Next	This opens the **Attestation Escalation Approval – Approvals**. Use this button to display an overview of all approvals made and set further options (see Granting or denying escalated attestation cases on page 194). As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 231: Controls in the attestation case's details pane

Control	Description
Actions > Go to attested object	Use this action to switch to an overview of the object to be attested (see Displaying escalated attestation cases on page 192).
Actions > Send inquiry	Use this action to send an inquiry to an identity about the attestation case (see Submitting inquiries about escalated attestation cases on page 198).
Actions > Reroute approval	Use this action to let another approval level make the approval decision about the attestation case. For example, if approval is required by a manager in a one-off case (see Rerouting approvals of escalated attestation cases on page 195).
Actions > Add approver	Use this action to add an additional approver to share the approval decision about the attestation case (see Appointing additional approvers to escalated attestation cases on page 196).
Actions > Delegate	Use this action to delegate the approval decision about the attestation

Control	Description
approval	case to another identity (see Delegating approvals of escalated attestation cases to other identities on page 197). You can revoke this action in the attestation history (see Withdrawing delegations from escalated attestation case approvals on page 198).
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of escalated attestation cases on page 166). Then you can send them reminder mails (see Sending reminders about escalated attestation cases on page 173).
Withdraw additional approval	If you have appointed an additional approver for this attestation case (see Appointing additional approvers to escalated attestation cases on page 196), use this button to revoke the action. Then you are the only approver of this attestation case again (see Removing additional approvers from escalated attestation cases on page 196).
Revoking hold status	Use this button to release the attestation case for approval again so that it can be processed by the approvers (see Revoking the hold status of escalated attestation cases on page 200).
Report	Use this button to generate a report about the object to attest.
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying escalated attestation cases on page 192).

Table 232: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new.

Column	Description
	It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Approval	Use these two buttons to make an approval decision about the attestation (see Granting or denying escalated attestation cases on page 194). TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

Attestation escalation – Approvals (page description)

To open the **Attestation Escalation Approval – Approvals** page go to **Attestation** > **Escalation** > Click an attestation policy > Make approval decision > **Next**.

After you have made your approval decisions on the **Attestation Escalation Approvals** page, you can save the approval decisions on the **Pending Attestation Approval – Approvals** page so that they take effect. You can also enter reason for the approval decisions here. For more information, see Granting or denying escalated attestation cases on page 194.

The following tables give you an overview of the various features and content on the **Attestation Escalation Approval – Approvals** page.

Table 233: Controls

Control	Description
Reason for approvals	Enter a reason for all approved attestations here.
Standard reason	Here you can select one of the standard reasons saved in the system

Control	Description
	for all approved attestations.
Reason for denials	Enter a reason for all denied attestations here.
Standard reason	Here you can select one of the standard reasons saved in the system for all denied attestations.
Save	Use this button to save all the settings and approval decisions.
Back	Use this button to switch to the previous page. For example, to approve other attestations.

Table 234: Columns

Column	Description
Display name	Shows you the name of the object to be attested.
Attestation policy	Shows the name of the attestation policy in use.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Reason	Here you can enter a reason for the decision. To do this, click on the button and, in the dialog, enter a reason or select one of the standard reasons.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance (Menu description)

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an employee is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.

- Each item that an identity access can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule and violations appear in the identity's Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information. For more information, see What statistics are available? on page 800.

You can use items on the **Compliance** menu to perform various actions and collect information. The following tables provide you with an overview of the menu items and actions that can be run here.

Table 235: Menu items

Menu	Menu item		Description
Compliance			
	My actions		
		Pending Rule Violations	Here you can make approval decisions about pending rule violations.
		Rule Violation History	Here you can display all the approvals that you made about rule violations.
		Pending Policy Violations	Here you can make approval decisions about pending policy violations.
		Policy Violation History	Here you can display all the approvals that you made about policy violations.
	Auditing		
		Rule Violations	Here you can display all rule violations.
		Policy Violations	Here you can display all policy violations.
	Governance administration		
		Risk assessment	Here you can display and edit all risk index functions.
		Compliance	Here you can display all compliance frameworks.

Menu	Menu item		Description
		frameworks	
		High-risk overview	Here you can display objects (for example, identities) with increased risk index.
		Rule violations	Here you can display all the compliance rules and corresponding rule violations.
		Policy violations	Here you can display all the company policies and corresponding policy violations.
		Rule analysis	Here you can display all compliance rules with SAP functions and the user accounts that violate these rules.
		Function analysis	Here you can display rule violations of identities assigned to critical SAP functions.

My actions (page description)

To open the **My Actions** page go to **Compliance** > **My Actions**.

On the **My Actions** page, you can perform various actions regarding compliance.

To do this, click on one of the tiles:

Table 236: Tiles

Tiles	Description
Pending rule violations	You select the following actions: • Show rule violations that have not been approved yet (see Displaying approvable rule violations on page 202) • Grant or deny rule exceptions (see Granting and denying rule violation exceptions on page 202) • Resolve rule violations (see Resolving rule violations on page 204)
Rule Violation History	Here you can view all the rule violations you have approved or denied in the past (see Displaying rule violation history on page 205).
Pending Policy Violations	You select the following actions: • Show policy violations that have not been approved yet (see Displaying approvable policy violations on page 206) • Permit or reject policy exceptions (see Approving and denying policy violations on page 206)

Tiles	Description
Policy Violation History	Here you can view all the policy violations you have approved or denied in the past.

Pending rule violations (page description)

To open the **Pending Rule Violations** page go to **Compliance** > **My Actions** > **Pending Rule Violations**.

On the **Pending Rule Violations** page, you can:

- Show rule violations that have not been approved yet (see Displaying approvable rule violations on page 202)
- Grant or deny rule exceptions (see Granting and denying rule violation exceptions on page 202)
- Resolve rule violations (see Resolving rule violations on page 204)

> TIP If you are an auditor or an approver, you can obtain more information about exception approvals from **Auditing** menu.

The following tables give you an overview of the various features and content on the **Pending Rule Violations** page.

Table 237: Controls

Control	Description
Approve	Use this button to grant the rule violation approval (see Granting and denying rule violation exceptions on page 202).
Deny	Use this button to deny the rule violation approval (see Granting and denying rule violation exceptions on page 202).
Next	Opens the **Exception approvals** page (see Exception approvals (page description) on page 993). Use this button to display an overview of all approvals made and set further options. As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 238: Controls in the details pane of a rule violation

Control	Description
Valid until	You can use this option to define until when this approval decision is valid (see Granting and denying rule violation exceptions on page 202).
Resolve	Use this button to resolve the rule violation. When resolving the rule

Control	Description
	violation, you have the option of removing individual entitlements (see Resolving rule violations on page 204).

Table 239: Columns

Column	Description
Employee	Shows you the name of the identity that violated the rule.
Rule violation	Shows you the name of the violated rule.
Approval state	Shows you what status the rule violation currently has. The following status' are possible: • **Approval decision pending**: The rule violation has yet to be decided. • **Exception granted**: The exception was approved. In the details pane, on the **Rule violation** tab, you can see why the exception was granted approval. • **Exception denied**: The exception was denied. In the details pane, on the **Rule violation** tab, you can see why the exception was denied approval.
Risk index (reduced)	Shows you the risk index reduced by the mitigating control.
Approval	Use these two buttons to make an approval decision about the attestation case. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Rule violation**: Shows you general information about the rule violation.
- **Rule**: Show general information about rule that was violated.

Exception approvals (page description)

To open the **Exception approvals** page go to **Compliance** > **My Actions** > **Pending Rule Violations** > Make approval decision > **Next**.

After you have made your approval decisions on the **Pending Rule Violations** page, you can save the approval decisions on the **Exception Approvals** page so that they take effect (see Granting and denying rule violation exceptions on page 202). You can also enter reason for the approval decisions here.

The following tables give you an overview of the various features and content on the **Exception approvals** page.

Table 240: Controls

Control	Description
Reason for approvals	Here you can enter a reason for all approved rule violations.
Standard reason	Here you can select one of the standard reasons saved in the system for all approved rule violations.
Reason for denials	Here you can enter a reason for all denied rule violations.
Standard reason	Here you can select one of the standard reasons saved in the system for all denied rule violations.
Save	Use this button to save all the settings and approval decisions.
Back	Use this button to switch to the previous page. For example, to approve other rule violations.

Table 241: Columns

Column	Description
Employee	Shows you the name of the identity that violated the rule.
Rule violation	Shows you the name of the rule that violates the identity.
Reason	Here you can enter a reason for the decision. To do this, click on the button and, in the dialog, enter a reason or select one of the standard reasons.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Rule Violation History (page description)

To open the **Rule Violation History** page go to **Compliance** > **My Actions** > **Rule Violation History**.

On the **Rule Violation History** page, you can view all the rule violations you have approved or denied in the past (see Displaying rule violation history on page 205).

The following table gives you an overview of the various features on the **Rule Violation History** page.

Table 242: Columns

Column	Description
Employee	Shows you the name of the identity that violated the rule.
Rule violation	Shows you the name of the violated rule.
Approval state	Shows you whether the exception was approved or denied. The following status' are possible: • **Exception granted**: The exception was approved. In the details pane, on the **Rule violation** tab, you can see why the exception was granted approval. • **Exception denied**: The exception was denied. In the details pane, on the **Rule violation** tab, you can see why the exception was denied approval.
Risk index (reduced)	Shows you the risk index reduced by the mitigating control.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Rule violation**: Shows you general information about the rule violation.
- **Rule**: Shows you general information about the rule that was violated.

Pending policy violations (page description)

To open the **Pending Policy Violations** page go to **Compliance** > **My Actions** > **Pending Policy Violations**.

On the **Pending Policy Violations** page, you can:

- Show policy violations that have not been approved yet (see Displaying approvable policy violations on page 206)
- Permit or reject policy exceptions (see Approving and denying policy violations on page 206)

TIP If you are an auditor or an approver, you can obtain more information about exception approvals from **Auditing** menu.

The following tables give you an overview of the various features and content on the **Pending Policy Violations** page.

Table 243: Controls

Control	Description
Approve	Use this button to grant exception approval (see Granting and denying rule violation exceptions on page 202).
Deny	Use this button to deny exception approval (see Granting and denying rule violation exceptions on page 202).
Next	Opens the **Exception approvals** page (see Exception approvals (page description) on page 997). Use this button to display an overview of all approvals made and set further options. As long as you have not made a decision (with the help of the previous buttons) this button is disabled.

Table 244: Columns

Column	Description
Violating object	Shows you the name of the object that violates the policy. TIP: In the details pane, on the **Object** tab, you can see additional information about the object.
Policy	Shows you the name of the violated policy.
Status	Shows you the current status of the policy violation. The following status' are possible: • **Approval decision pending**: The policy violation has yet to be decided. • **Exception granted**: The exception was approved. In the details pane, on the **Policy violation** tab, you can see why the exception was granted approval. • **Exception denied**: The exception was denied. In the details pane, on the **Policy violation** tab, you can see why the exception was denied approval.
Approval	Use these two buttons to make an approval decision about the policy violation. TIP: If you have made all your approval decisions, click **Next** to open an overview page and save all the approvals.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: On the following tabs in the details pane, you can view other useful information about each rule violation. To do this, click the corresponding entry in the list.

- **Policy violation**: Shows you general information about the policy violation.
- **Object**: Shows you general information about object that was violated the policy.
- **Policy**: Shows you general information about policy that was violated.

Exception approvals (page description)

To open the **Exception approvals** page go to **Compliance** > **My Actions** > **Pending Policy Violations** > Make approval decision > **Next**.

After you have made your approval decisions on the **Pending Policy Violations** page, you can save the approval decisions on the **Exception Approvals** page so that they take effect (see Approving and denying policy violations on page 206). You can also enter reason for the approval decisions here.

The following tables give you an overview of the various features and content on the **Exception approvals** page.

Table 245: Controls

Control	Description
Reason for approvals	Here you can enter a reason for all approved policy violations.
Standard reason	Here you can select one of the standard reasons saved in the system for all approved policy violations.
Reason for denials	Here you can enter a reason for all denied policy violations.
Standard reason	Here you can select one of the standard reasons saved in the system for all denied policy violations.
Save	Use this button to save all the settings and approval decisions.
Back	Use this button to switch to the previous page. For example, to approve other policy violations.

Table 246: Columns

Column	Description
Violating object	Shows you the name of the object that violates the policy.
Policy	Shows you the name of the policy that violates the object.
Reason	Here you can enter a reason for the decision. To do this, click on the button and, in the dialog, enter a reason or select one of the standard reasons.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Policy violations (page description)

To open the **Policy Violations** page go to **Compliance** > **My Actions** > **Policy Violations**.

On the **Policy Violations** page, you can view all the policy violations you have approved or denied in the past (see Displaying policy violation history on page 207).

The following table gives you an overview of the various features on the **Policy Violations** page.

Table 247: Columns

Column	Description
Violating object	Shows you which object violated the policy.
Policy	Shows you the name of the violated policy.
State	Shows you whether the exception was approved or denied. The following status' are possible: • **Exception granted**: The exception was approved. In the details pane, on the **Policy violation** tab, you can see why the exception was granted approval. • **Exception denied**: The exception was denied. In the details pane, on the **Policy violation** tab, you can see why the exception was denied approval.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: On the following tabs in the details pane, you can view other useful information about each rule violation. To do this, click the corresponding entry in the list.

- **Policy violation**: Shows you general information about the policy violation.
- **Object**: Shows you general information about object that was violated the policy.
- **Policy**: Shows you general information about policy that was violated.

Auditing (page description)

To open the **Auditing** page go to **Compliance** > **Auditing**.

On the **Auditing** page, you can display all the approval decisions about rule and policy violations in the system.

To do this, click on one of the tiles:

Table 248: Tiles

Tiles	Description
Rule violations	Here you can display all rule violations.
Policy violations	Here you can display all policy violations.

Auditing - rule violations (page description)

To open the **Auditing – Rule Violations** page go to **Compliance** > **Auditing** > **Rule Violations**.

On the **Auditing – Rule Violations** page you can view all rule violations in the system (see Displaying all rule violations on page 208).

The following tables give you an overview of the various features and content on the **Auditing – Rule Violations** page.

Table 249: Controls

Control	Description
Select approver	Click **Assign** and select the identity whose approvals you want to display.

Table 250: Columns

Column	Description
Employee	Shows you the name of the identity that violated the rule.
Rule violation	Shows you the name of the violated rule.
Approval state	Shows you what status the rule violation currently has. The following status' are possible: • **Approval decision pending**: The rule violation has yet to be decided. • **Exception granted**: The exception was approved. In the details pane, on the **Rule violation** tab, you can see why the exception was granted approval. • **Exception denied**: The exception was denied. In the details pane, on the **Rule violation** tab, you can see why the exception was denied approval.
Risk index (reduced)	Shows you the risk index reduced by the mitigating control.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Rule violation**: Shows you general information about the rule violation.
- **Rule**: Show general information about rule that was violated.

Auditing – Policy violations (page description)

To open the **Auditing – Policy Violations** page go to **Compliance** > **Auditing** > **Policy Violations**.

On the **Auditing - Policy Violations** page, you can display all policy violations in the system (see Displaying all policy violations on page 208).

The following tables give you an overview of the various features and content on the **Auditing – Policy Violations** page.

Table 251: Controls

Control	Description
Select approver	Click **Assign** and select the identity whose approvals you want to display.

Table 252: Columns

Column	Description
Employee	Shows you the name of the identity that violated the policy.
Policy	Shows you the name of the violated policy.
State	Shows you the current status of the policy violation. The following status' are possible: • **Approval decision pending**: The policy violation has yet to be decided. • **Exception granted**: The exception was approved. In the details pane, on the **Policy violation** tab, you can see why the exception was granted approval. • **Exception denied**: The exception was denied. In the details pane, on the **Policy violation** tab, you can see why the exception was denied approval.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: On the following tabs in the details pane, you can view other useful information about each rule violation. To do this, click the corresponding entry in the list.

- **Policy violation**: Shows you general information about the policy violation.
- **Object**: Shows you general information about object that was violated the policy.
- **Policy**: Shows you general information about policy that was violated.

Governance administration (page description)

To open the **Governance Administration** page go to **Attestation** > **Governance Administration**.

On the **Governance Administration** page, you can manage compliance rules and company policies and related functions.

To do this, click on one of the tiles:

Table 253: Tiles

Tiles	Description
Risk assessment	Here you can perform the following actions for the risk index functions that contribute to the calculation of risk indexes: • Show risk index functions (see Displaying risk index functions on page 210) • Edit risk index functions (see Editing risk index functions on page 210) • Enable risk index functions (see Enabling/disabling risk index functions on page 211) • Disable risk index functions (see Enabling/disabling risk index functions on page 211)
Compliance framework	Here you can display all compliance frameworks (see Displaying compliance frameworks on page 212).
High-risk overview	Here you can see an overview of the objects with the highest risk factor (see Displaying high risk objects on page 800).
Rule violations	Here you can get an overview of compliance rules and the corresponding rule violations and generate detailed reports on them (see Displaying compliance rules and rule violations on page 213).
Policy violations	Here you can get an overview of company policies and the corresponding policy violations, and generate detailed reports about them (see Displaying company policies and violations on page 215).

Tiles	Description
Rule analysis	Here you can display all compliance rules with SAP functions and the user accounts that violate them (see Displaying compliance rules with SAP functions on page 216). You can investigate the rule violation to determine the reason for it and take action if necessary.
Function analysis	Here you can display all rule violations of identities assigned to critical SAP functions (see Displaying rule violations of identities with critical SAP functions on page 217).

Risk assessment (page description)

To open the **Risk Assessment** page go to **Compliance** > **Governance Administration** > **Risk Assessment**.

Everyone with IT system authorization in a company represents a security risk for that company. For example, a person with permission to edit financial data in SAP carries a higher risk than an employee with permission to edit their own personal data. To quantify the risk, you can enter a risk value for every company resource in One Identity Manager. A risk index is calculated from this value for every person who is assigned this company resource, directly, or indirectly. Company resources include target system entitlements (for example, Active Directory groups or SAP profiles), system roles, subscribable reports, software, and resources. In this way, all the people that represent a particular risk to the company can be found.

In the context of Identity Audit, compliance rules can also be given a risk index. With each rule violation, the security risk of all identities that violate the rule may increase. Therefore, these risk indexes are also included in the identities' risk calculation. You can define appropriate countermeasures through mitigating controls, and store them with the compliance rules.

Other factors can influence the calculation of identities' risk indexes. These include: the type of resource assignment (approved request or direct assignment), attestations, exception approvals for rule violations, identity's responsibilities, and defined weightings. Furthermore, the risk index can be calculated for all business roles, organizations, and system roles that have company resources assigned to them. The user account risk index is calculated based on the system entitlements assigned.

For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

On the **Risk Assessment** page, you can perform the following actions for the risk index functions that contribute to the calculation of these indexes:

- Show risk index functions (see Displaying risk index functions on page 210)
- Edit risk index functions (see Editing risk index functions on page 210)
- Enable risk index functions (see Enabling/disabling risk index functions on page 211)
- Disable risk index functions (see Enabling/disabling risk index functions on page 211)

The following table gives you an overview of the various features on the **Risk Assessment** page.

Table 254: Columns

Column	Description
Object type	Shows you which objects are affected by the risk index function.
Name	Shows you the risk index function's name.
Calculation type	Shows you the calculation type used for risk assessment. The following calculation types are possible: • **Maximum (weighted)**: The highest value from all relevant risk indexes is determined, weighted and used as the basis for further calculation. • **Maximum (normalized)**: The highest value from all relevant risk indexes is calculated, weighted with the normalized weighting factor and taken as basis for the next calculation. • **Increment**: The risk index of table column (target) is incremented by a fixed value. You can see this value in the **Weighting/Change value** column. • **Decrement**: The risk index of the table column (target) is decreased by a fixed value. You can see this value in the **Weighting/Change value** column. • **Average (normalized)**: The average of all relevant risk indexes is calculated with the normalized weighting factor and taken as basis for the next calculation. • **Average (weighted)**: The average of all relevant risk indexes is calculated, weighted, and taken as basis for the next calculation. • **Reduction**: Used when calculating the reduced risk index for compliance rules, SAP functions, company policies, and attestation policies. You cannot add custom functions with this calculation type!
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance frameworks (page description)

To open the **Compliance Frameworks** page go to **Compliance** > **Governance Administration** > **Compliance Frameworks**.

Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements.

On the **Compliance Frameworks** page, you can display all the compliance frameworks (see Displaying compliance frameworks on page 212).

The following table gives you an overview of the various features on the **Compliance Frameworks** page.

Table 255: Columns

Column	Description
Name	Shows you the compliance framework's name.
Description	Shows you a description of the compliance framework.
Manager/supervisor	Shows you who is responsible for the compliance framework.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance framework details (page description)

To open the **Compliance Frameworks** page go to **Compliance** > **Governance Administration** > **Compliance Frameworks** > click list entry.

On the **Compliance Frameworks** page, you will see a overview of a specific compliance framework displayed as a HyperView (after you select it on the **Compliance Frameworks** page) and you can create a report listing the compliance framework's rule violation (see Displaying compliance frameworks on page 212).

The following table gives you an overview of the various features on the **Compliance Frameworks** page.

Table 256: Controls

Control	Description
Rule overview report	Use this button to generate a report about the compliance framework's rule violations.

High risk overview (page description)

To open the **High Risk Overview** page go to **Compliance** > **Governance Administration** > **High Risk Overview**.

On the **High Risk Overview** page, you can get overview of the objects with the highest risk factor (see Displaying high risk objects on page 800). This can help you prioritize when managing your business resources. Company resources have risk values, which provide the risk index when combined with risk index functions.

The following tables give you an overview of the various features and content on the **High Risk Overview** page.

Table 257: Controls

Control	Description
Show all high risk objects	Select this check box if you want to show all the high risk objects (instead of just the top 10) (see Displaying high risk objects on page 800).

Table 258: Columns

Column	Description
High Risk Objects	
Display name	Shows you the object's display name.
Object type	Shows you the type of object.
Risk index	Show the object's risk index.
High Risk Employees	
Full name	Shows the identity's name.
Primary department	Shows you to which department the identity is primarily assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
High Risk Business roles	
Business role	Shows the business role's name.
Role class	Shows the business role's role class.
Risk index (calculated)	Shows you the business role's calculated risk index.
High Risk System roles	
System role	Shows the system role's internal name.

Column	Description
Display name	Shows the system role's display name.
System role manager	Shows you the name of the identity responsible for the system role.
Risk index (calculated)	Shows you the system role's calculated risk index.
High Risk System entitlements	
Display	Shows the system entitlement's display name.
Group type	Shows the system entitlement's group type.
Risk index	Shows the system entitlement's risk index.
High Risk User accounts	
Login name	Shows you the user name of the user account used to log in.
Name	Shows you the user account's display name.
Employee	Shows you the name of the identity to which the user account is primarily assigned.
Container	Shows you in which container the user account is located.
Risk index (calculated)	Shows you the calculated user account's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Rule violations (page description)

To open the **Rule Violations** page go to **Compliance** > **Governance Administration** > **Rule Violations**.

On the **Rule Violations** page, you get an overview of compliance rules and the corresponding rule violations and generate detailed reports on them (see Displaying compliance rules and rule violations on page 213). This information can help to determine gaps in your security or compliance policies and to develop attestation policies or mitigating controls. Mitigating controls are processes existing outside the One Identity Manager solution and reduce the risk of violation.

The following tables give you an overview of the various features and content on the **Rule Violations** page.

Table 259: Controls

Control	Description
By framework	Enable this option to display all compliance rules associated with compliance frameworks for which you are responsible.
By department	Enable this option to display all compliance rules violated by identities belonging to departments for which you are responsible.
By rule	Enable this option to display all compliance rules for which you are responsible.
By approval role	Enable this option to display all compliance rules for which you are allowed to grant exceptions.
All compliance rules	Enable this option to display all compliance rules.

Table 260: Controls in the detail pane of a compliance rule

Control	Description
Show details	This opens the **<rule>** page (see Rule details (page description) on page 1008). Use this button to display more details about the compliance rule as a HyperView (see Displaying compliance rules and rule violations on page 213).
Report	Use this button to generate a report listing the rule violations (see Displaying compliance rules and rule violations on page 213). The report contains a risk assessment for you to use for prioritizing violations and on which to base subsequent planning. The risk assessment takes into account many risk factors that arise from violations and represents the risk as a value between 0 (no risk) and 1 (high risk).

Table 261: Columns

Column	Description
Rule name	Shows you the compliance rule's name.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more

Column	Description
	information, see Compliance – Governance Administration on page 209.
Rule violations (new)	Shows you how often the compliance rule has been violated recently.
Rule violations (all)	Shows you how often the compliance rule is violated.
Rule group	Shows you the rule group to which the compliance rule belongs based on its content.
Compliance framework	Shows you the compliance framework to which the compliance rule belongs.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: You can see more information about each compliance rule in the details pane. To do this, click the corresponding entry in the list.

Rule details (page description)

To open the **<rule name>** details page go to **Compliance** > **Governance Administration** > **Rule Violations** > click an entry in the list.

On the **<rule name>** details page, you will see a overview of a specific company policy displayed as a HyperView (after you select Show Details on the **Rule violations** page) and you can create a report listing the rule violations.

The following table gives you an overview of the various features on the **<rule name>** details pane.

Table 262: Controls

Control	Description
Report	Use this button to generate a report listing the rule violations. The report contains a risk assessment for you to use for prioritizing violations and on which to base subsequent planning. The risk assessment takes into account many risk factors that arise from violations and represents the risk as a value between 0 (no risk) and 1 (high risk).

Policy violations (page description)

To open the **Policy Violations** page go to **Compliance** > **Governance Administration** > **Policy Violations**.

On the **Policy Violations** page, you get an overview of company policies and the corresponding policy violations, and generate detailed reports about them (see Displaying company policies and violations on page 215). This information can help to determine gaps in your security or compliance policies and to develop attestation policies or mitigating controls. Mitigating controls are processes existing outside the One Identity Manager solution and reduce the risk of violation.

The following tables give you an overview of the various features and content on the **Policy Violations** page.

Table 263: Controls

Control	Description
For framework owners	Enable this option to display all company policies associated with compliance frameworks for which you are responsible.
For policy owners	Enable this option to display all company policies for which you are responsible.
For exception approvers	Enable this option to display all company policies for which you are allowed to grant exceptions.
All policies	Enable this option to display all company policies.

Table 264: Controls in the company policy's details pane

Control	Description
Show details	This opens the **<policy> (Policy)** page (see Policy details (page description) on page 1010). Use this button to display more details about the company policy as a HyperView (see Displaying company policies and violations on page 215).
Report	Use this button to generate a report listing the policy violations (see Displaying company policies and violations on page 215). The report contains a risk assessment for you to use for prioritizing violations and on which to base subsequent planning. The risk assessment takes into account many risk factors that arise from violations and represents the risk as a value between 0 (no risk) and 1 (high risk).

Table 265: Columns

Column	Description
Policy	Shows you the name of the company policy.
Risk index	Shows the severity of the policy violation (meaning the calculated risk index). The higher this value is, the higher the risk that this policy violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. The risk of a policy violation can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of a policy violation. For more information, see Compliance – Governance Administration on page 209.
Policy violations (new)	Shows you how often the company policy has been violated recently.
Policy violations (all)	Shows you how often the company policy is violated.
Policy group	Shows you the policy group to which the company policy belongs, based on its content.
Compliance framework	Shows you the compliance framework to which the company policy belongs.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: You can see more information about each company policy in the details pane. To do this, click the corresponding entry in the list.

Policy details (page description)

To open the **<policy name>** details page go to **Compliance** > **Governance Administration** > **Policy Violations** > click an entry in the list.

On the **<policy name>** details page, you will see a overview of a specific company policy displayed as a HyperView (after you select Show Details on the **Policy violations** page) and you can create a report listing the policy violations.

The following table gives you an overview of the various features on the **<policy name>** details pane.

Table 266: Controls

Control	Description
Report	Use this button to generate a report listing the policy violations. The report contains a risk assessment for you to use for prioritizing violations and on which to base subsequent planning. The risk assessment takes into account many risk factors that arise from violations and represents the risk as a value between 0 (no risk) and 1 (high risk).

Rule analysis (page description)

To open the **Rule Analysis** page go to **Compliance** > **Governance Administration** > **Rule Analysis**.

Identities who have access to certain critical SAP functions, may violate compliance rules and can pose a significant security threat. On the **Rule Analysis** page, you can display all compliance rules with the SAP functions and user accounts that violate them (see Displaying compliance rules with SAP functions on page 216). You can investigate the rule violation to determine the reason for it and take action if necessary.

If you click a compliance rule in the list, a new page opens (see Rule Analysis – Rule (page description) on page 1011) displaying the user accounts and identities violate that rule (see Displaying compliance rules with SAP functions on page 216).

The following table gives you an overview of the various features on the **Rule Analysis** page.

Table 267: Columns

Column	Description
Rule	Shows you the compliance rule's name.
Description	Shows you the compliance rule's description.
Significance	Shows you how high the risk is if this compliance rule is violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Rule Analysis – Rule (page description)

To open the **Rule Analysis – Rule** page go to **Compliance** > **Governance Administration** > **Rule Analysis** > Click a rule.

On the **Rule Analysis - Rule** page you can examine a rule violation selected on the **Rule Analysis** page (see Rule analysis (page description) on page 1011) to find the reason for it and take any necessary measures (see Displaying compliance rules with SAP functions on page 216).

The following table gives you an overview of the various features on the **Rule Analysis – Rule** page.

Table 268: Columns

Column	Description
User account	Shows you the name of the SAP user account that violates the compliance rule.
Employee	Shows you the name of the identity that violates the compliance rule.
Analyze rule violation	Click **By role** to display details of the rule violation roles and profiles. Click **By ability** to display details of SAP functions and transactions.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Rule violations by user (page description)

To open the **Rule Violations** page go to **Compliance** > **Governance Administration** > **Critical Function Analysis**.

On the **Rule Violations by User** page, you can display all rule violations of identities associated with critical SAP functions (see Displaying rule violations of identities with critical SAP functions on page 217).

Clicking an identity in the list opens a new page (see Rule violations for an identity (page description) on page 1013) that displays critical SAP functions and rule violations of the corresponding identity (see Displaying rule violations of identities with critical SAP functions on page 217).

The following table gives you an overview of the various features on the **Rule Violations by User** page.

Table 269: Columns

Column	Description
Full name	Shows you the name of the identity that violates the compliance rule.
Central SAP user account	Shows you the name of the central SAP user account that the identity uses.
Primary department	Shows you the primary department of identity that violates the compliance rule.
Functional area	Shows you the functional area of the identity that violates the compliance rule.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Rule violations for an identity (page description)

To open the **Rule Violations for <identity>** page go to **Compliance** > **Governance Administration** > **Critical Function Analysis** > click an identity.

On the **Rule Violations for <identity>** page, you can investigate an identity to determine the reason for a rule violation and take action if necessary (see Displaying rule violations of identities with critical SAP functions on page 217).

Here you can find out which of the identity's SAP functions was involved in the violation and the rules that caused the violation.

The following table gives you an overview of the various features on the **Rule Violations for <identity>** page.

Table 270: Columns

Column	Description
SAP functions from ...	
Function definition	Shows you the identity's SAP function name.
Description	Shows you the identity's SAP function description.
Significance	Shows you how high the risk of this SAP function is.
Rule violations by ...	
Rule number	Shows you the rule number of the compliance rule that the identity violates.
Rule	Shows you the name of the compliance rule that the identity violates.
Description	Shows you the description of the compliance rule that the identity violates.
Significance	Shows you how high the risk of this rule violation is.
Functions	Shows you the identity's SAP function name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Responsibilities (Menu description)

You can use items on the **Responsibilities** menu to perform various actions and collect information about responsibilities. The following tables provide you with an overview of the menu items and actions that can be run here.

Table 271: Menu items

Menu	Menu item		Description
Ownerships			
	My responsibilities		Here you can manage objects that you are responsible for within your company.
	Delegation		
		Delegation	Here you can delegate responsibilities to other identities.
		Delegation history	Here you can display your past delegations made.
	Ownerships		
		Assigning owners	Here you can assign owners to objects.
		Claim ownership	Here you can request responsibility for a group.
	Auditing		Here you can display all objects in the system and their details.
	Governance administration		Here you can manage all objects in the system.

My responsibilities (page description)

To open the **My Responsibilities** page go to **Responsibilities** > **My Responsibilities**.

On the **My Responsibilities** page, you can manage the objects that you are responsible for within your company.

To do this, click on one of the tiles:

- Identities
- System entitlements
- Business roles
- System roles
- Departments
- Cost centers
- Locations

- One Identity Manager application roles
- Resources
- Assignment resources
- Multi-request resources
- Software
- Multi requestable/unsubscribable resources
- Devices

Identities (page description)

To open the **Identities** page go to **Responsibilities** > **My Responsibilities** > **Identities**.

On the **Identities** page, you can:

- View all the identities that you manage (see Displaying my identities on page 300)
- Add new identities (see Adding your own identities on page 301)
- Show your identities' rule violations (see Displaying my identities' rule violations on page 302)

If you click an identity in the list, a new page opens (see Identity overview page (page description) on page 1018), which contains more information and configuration options for the identity.

The following tables give you an overview of the different functions and content on the **Identities** page.

Table 272: Controls

Control	Description
Show only direct reports	Select the check box if you to show only identities that report directly to you. To show all the identities that you manage (indirectly too), do not select the check box.
Rule violations	Opens the **Rule violations by direct reports** page (see Rule violations of directly subordinated identities (page description) on page 1016). Use this button to show all the rule violations of all identities that report to you (see Displaying my identities' rule violations on page 302).
Add a new identity	Opens the **Add a New Identity** page (see Adding a new identity (page description) on page 1017). Use this button to add a new identity to the system (see Adding your own identities on page 301).

Table 273: Columns

Column	Description
Display	Shows the identity's name.
Primary department	Shows the department that the identity is primarily assigned to.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Rule violations of directly subordinated identities (page description)

To open the **Rule violations of directly subordinated identities** page go to **Responsibilities** > **My Responsibilities** > **Identities** > **Rule Violations**.

On the **Rule Violations of Directly Subordinate Identities** page you can view all rule violations of identities that report directly to you (see Displaying my identities' rule violations on page 302).

The following table gives an overview of the various content of the **Rule violations of directly subordinated identities** page.

Table 274: Columns

Column	Description
Employee	Shows you the name of the identity causing the rule violation.
Rule violation	Shows you the name of the compliance rule that the identity violates.
Checked	Shows whether the rule violation was tested.
Exception is approved	Shows you whether an exception was approved for the rule violation.
Risk index (calculated)	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.
Approval date	Shows you when an approval decision about the rule violation was made.
Reason	Shows you the reason for the rule violation decision.

Adding a new identity (page description)

To open the **Add a New Identity** page go to **Responsibilities** > **My Responsibilities** > **Identities** > **Add a new identity**.

On the **Add a New Identity** page, you can create a new identity for which you are responsible. Do this by entering the new identity's main data (see Adding your own identities on page 301).

Enter the following main data.

Table 275: Identities main data

Property	Description
Personal data	
Last name	Enter the identity's last name.
First name	Enter the identity's first name.
Middle name	Enter the identity's middle name.
Date of birth	Enter the identity's date of birth. Click the (**Calendar**) to do this and use the date picker to select the date of birth.
Personnel number	Enter the identity's personnel number.
Gender	In the menu, select the identity's gender.
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Organizational information	
Primary cost center	Click **Assign**/**Change** and select the identity's primary cost center.
Primary department	Click **Assign**/**Change** and select the identity's primary department.
External	Select the check box if this is an external identity.
Employee type	In the menu, select what type of identity this is. For example, an identity of this company or a trainee.
Entry date	Enter the date the identity started at the company. Click the (**Calendar**) and use the date picker to select the starting date.
Leaving date	Enter the date that the identity leaves the company. Click the (**Calendar**) to do this and use the date picker to select the leaving date.
Manager	Shows you the identity's manager.

Property	Description
	TIP: If necessary, you can transfer the identity's manager at a later date (see Assigning other managers to my identities on page 299).
Primary location	Click **Assign/Change** and select the identity's primary location.
Building	Enter the building where the identity works.
Floor	Enter which floor the identity works on.
Room	Enter the room the identity works in.
Street	Enter the road where the identity works.
Zip code	Enter the zip code of the identity's work location.
City	Enter the city where the identity works.

Identity overview page (page description)

To open an identity's overview page go to **Responsibilities** > **My Responsibilities** > **Identities** and click an identity.

On the identity's overview page, you can perform various actions on the identity you selected beforehand.

To do this, click on one of the tiles:

Table 276: Tiles

Tile	Description
Overview	Opens the **Overview - Identity** page (see Overview – Identity (page description) on page 1020). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my identities' overviews on page 303). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data – Identity** page (see Main data – Identity (page description) on page 1020). Here you can see and edit the identity's main data (see Displaying and editing my identities' main data on page 301).
Permissions	Opens the **Entitlements – Identity** page (see Entitlements – Identity (page description) on page 1025). You select the following actions: • Display entitlements assigned to the identity (see Displaying my identities' entitlements on page 305)

Tile	Description
	• Remove the identity's entitlements (see Deleting my identities' entitlements on page 305)
My Requests	Opens the **Requests – Identity** page (see Requests - Identity ((page description)) on page 1023). Here you can see all the products that this identity has requested or were requested for them (see Displaying my identity requests on page 304).
Delegations	Opens the **Delegations – Identity** page (see Delegations – Identity (page description) on page 1026). You select the following actions: • Display all delegations that the identity is involved in (see Deleting my identities' delegations on page 306) • Delegate the identity's role memberships and responsibilities to other identities (see Adding delegations for my identities on page 307) • Cancel delegations (see Canceling my identities' delegations on page 307) • Delete delegations (see Deleting my identities' delegations on page 308)
Attestation	Opens the **Attestation – Identity** page (see Attestations – Identity (page description) on page 1027). You select the following actions: • Display all attestation cases linked to this identity (see Displaying attestation cases of my identities on page 309) • Display details of the objects being attested (see Displaying attestation cases of my identities on page 309) • Make approval decisions about pending attestation cases (see Approving and denying my identities' attestation cases on page 311) • Display attestors of pending attestation cases (see Displaying attestors of my identities' pending attestation cases on page 310) • Send reminders to approvers (see Sending reminders about my identities' pending attestation cases on page 312)
Risk	Opens the **Risk – Identity** page (see Risk – Identity (page description) on page 1029). Here you can see the identity's risk index (see Displaying my identities' risk indexes on page 314). For more information about risk assessment, see the Risk assessment on page 209.

Tile	Description
History	Opens the **History – Identity** page (see History – Identity (page description) on page 1030). Here you can see all the changes made to the identity (see My identities' history on page 315).
Passcode	Here you can create a passcode for the identity if it has forgotten its Web Portal login password and cannot reset it using the question-and-answer function (see Creating passcodes for my identities on page 300).

Overview – Identity (page description)

To open the **Overview – Identity** page go to **Responsibilities** > **My Responsibilities** > **Identities** > select identity> **Overview**.

On the **Overview - Identity** page, you can see all the information relevant to the identity summarized in an overview (see Displaying my identities' overviews on page 303).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Identity (page description)

To open the **Main data – Identity** page go to **Responsibilities** > **My Responsibilities** > **Identity** > select identity > **Main data**.

On the **Main data – Identity** page, you can:

- Display the identity's main data (see Displaying and editing my identities' main data on page 301)
- Edit the identity's main data (see Displaying and editing my identities' main data on page 301)
- Transfer the identity to another manager (see Assigning other managers to my identities on page 299)
- Create a report about the identity's data (see Creating reports about my identities on page 303)

The following tables give you an overview of the different functions and content on the **Main data – Identity** page.

Table 277: Controls

Control	Description
Assign to new manager	Opens the **Assign to New Manager** page (see Assigning to new manager (page description) on page 1022). Use this button to transfer the identity's responsibilities from themself to another manager (see Assigning other managers to my identities on page 299).

Control	Description
Generate report	Use this button to generate a report about the identity's data (see Creating reports about my identities on page 303).
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 278: Identities main data

Property	Description
Personal data	
Last name	Enter the identity's last name.
First name	Enter the identity's first name.
Middle name	Enter the identity's middle name.
Date of birth	Enter the identity's date of birth. Click the (**Calendar**) to do this and use the date picker to select the date of birth.
Personnel number	Enter the identity's personnel number.
Gender	In the menu, select the identity's gender.
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Organizational information	
Primary cost center	Click **Assign**/**Change** and select the identity's primary cost center.
Primary department	Click **Assign**/**Change** and select the identity's primary department.
External	Select the check box if this is an external identity.
Employee type	In the menu, select what type of identity this is. For example, an identity of this company or a trainee.
Entry date	Enter the date the identity started at the company. Click the (**Calendar**) and use the date picker to select the starting date.
Leaving date	Enter the date that the identity leaves the company. Click the (**Calendar**) to do this and use the date picker to select the leaving date.
Manager	Shows you the identity's manager. TIP: If necessary, you can transfer the identity's manager at a later

Property	Description
	date (see Assigning other managers to my identities on page 299).
Temporarily disable until	Select the check box to activate the identity at a later date then click the (**Calendar**) and use the date picker to select the date to activate the identity.
Locational information	
Primary location	Click **Assign**/**Change** and select the identity's primary location.
Building	Enter the building where the identity works.
Floor	Enter which floor the identity works on.
Room	Enter the room the identity works in.
Street	Enter the road where the identity works.
Zip code	Enter the zip code of the identity's work location.
City	Enter the city where the identity works.

Assigning to new manager (page description)

To open the **Assign to new manager** page go to **Responsibilities** > **My responsibilities** > **Identities** > click an identity > **Main data** > **Assign to new manager**.

On the **Assign to New Manager** page, you can assign a new manager to an identity and specify which changes to make on the day the manager takes effect (see Assigning other managers to my identities on page 299).

NOTE: By default, if the identity to which you want to assign a new manager already has approved requests or entitlements, these will be deleted on the deadline by default. If you want the identity to retain these requests or entitlements when transferring to the new manager, disable the check box in the column **Delete on the effective date** or **Cancel on the effective date**.

The following tables give you an overview of the various features and content on the **Assign to New Manager** page.

Table 279: Controls

Control	Description
New manager	Click **Assign**/**Change** and then select the identity's new manager.
Effective date	Enter the date on which the new manager will take over responsibility for the identity. Click **Calendar** to do this and use the date picker to select the date.
Back	Opens the **Main data – Identity** page (see Main data – Identity

Control	Description
	(page description) on page 1020).
Submit	Use this button to save your settings. The manager will be assigned to the identity on the specified date.

Table 280: Columns

Column	Description
Description	Shows you which change is to be made on the effective date.
Object type	Shows you what type of object it is that will be changed on the effective date.
Object	Shows you the name of the object that will be changed on the effective date.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Requests - Identity ((page description))

To open the **Requests – Identity** page go to **Responsibilities** > **My Responsibilities** > **Identities** > select identity > **Requests**.

On the **Requests - Identity** page you can view all the requests an identity has requested itself or that have been requested for them (see Displaying my identity requests on page 304).

The following tables give you an overview of the various features and content on the **Requests – Identity** page.

Table 281: Controls

Control	Description
Advanced search	The advanced search allows you to control which product requests are displayed: • **Requests submitted by the selected identity for itself**: Select this check box to display product requests placed by the selected identity for themselves. • **Requests submitted by the selected identity for others**: Select this check box to display product requests placed by the selected identity for other identities. • **Requests submitted by others for the selected identity**: Select this check box to display product requests placed by other identities for the selected identity. • **Submitted requests in the selected identity's**

Control	Description
	organization: Select this check box to display product requests placed in the selected identity's scope of responsibility. • **Filter by request number**: Enter the request number of the request you want to display. • **pending**: Select this check box to display product requests that are not yet approved (status: **Request**). • **Approved**: Select this check box to display product requests that have been granted approval (status: **Assigned**). • **Canceled or denied or unsubscribed**: Select this check box to display product requests that have been canceled, denied, or unsubscribed. Click **Search** to apply the filter criteria to the request history. Click **Reset** to reset the filter criteria to the default search.

Table 282: Columns

Column	Description
Product	Shows the name of the product that was requested.
State	Shows the current status of the product. The following status' are possible: • **Assigned**: The product request was successful and the product was successfully assigned. • **Request**: The product request is still awaiting an approval decision (it is still in the request workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The product request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The product request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Renewal**: The product has been renewed (see Renewing products with limit validity periods on page 130). • **Unsubscription**: The product is in the process of being unsubscribed (see Unsubscribing products on page 131). • **Denied**: The request for this product was denied. The reason for denying may be a policy or rule violation or the manager not verifying the request if it is only temporary. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. .

Column	Description
	• **Canceled**: The product request was canceled or the system could not carry out the request (for example, because an identity for verifying it was not given or the validity period expired). In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed**: The product was unsubscribed (see Unsubscribing products on page 131). In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested. TIP: If you only want to display products that were requested within a certain time period, click **Filtering: Request date** next to the column header and select the appropriate options.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows you the request number of the total request with which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Entitlements – Identity (page description)

To open the **Entitlements – Identity** page go to **Responsibilities** > **My Responsibilities** > **Identities** > select identity > **Entitlements**.

On the **Entitlements – Identity** page, you can:

- Display entitlements assigned to the identity (see Displaying my identities' entitlements on page 305)
- Remove the identity's entitlements (see Deleting my identities' entitlements on page 305)

The following tables give you an overview of the various features and content on the **Entitlements – Identity** page.

Table 283: Controls

Control	Description
Deleting memberships	Use this button to delete selected entitlements (such as, membership in groups) (see Deleting my identities' entitlements on page 305). To do this, select the check box in front of the entitlement and click the button.

Table 284: Columns

Column	Description
Entitlement	Shows the entitlement's name.
Object type	Shows the entitlement type (for example, if it is a system role)
Origin	Shows how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.

> TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Delegations – Identity (page description)

To open the **Delegations – Identity** page go to **Responsibilities** > **My Responsibilities** > **Identities** > select identity > **Delegations**.

On the **Delegations – Identity** page, you can:

- Display all delegations that the identity is involved in (see Deleting my identities' delegations on page 306)
- Delegate the identity's role memberships and responsibilities to other identities (see Adding delegations for my identities on page 307)
- Cancel delegations (see Canceling my identities' delegations on page 307)
- Delete delegations (see Deleting my identities' delegations on page 308)

The following tables give you an overview of the various features and content on the **Delegations – Identity** page.

Table 285: Controls

Control	Description
Actions > Delete all delegations	Use this action to delete all existing delegations that the identity has triggered (see Deleting my identities' delegations on page 308). NOTE: You cannot delete responsibilities that you have delegated to the identity here. Delete this delegation instead as described in Deleting delegations on page 461.
Actions > Delete	Use this action to delete delegations that you have previously selected

Control	Description
delegation	using the ☑ **Select** button (see Deleting my identities' delegations on page 308).
Actions > Select all	Use this action to select all the delegations and then delete them (see Deleting my identities' delegations on page 308).
Adding new delegations	Use this button to add a new delegation (see Adding delegations for my identities on page 307).

Table 286: Controls in the details pane of a delegation

Control	Description
Withdraw request	Use this button to cancel the selected delegation (see Canceling my identities' delegations on page 307).
Details	You can use this function to view details of all objects involved in the delegation (see Deleting my identities' delegations on page 306).

Table 287: Columns

Column	Description
Name	Shows you the name of the object whose responsibility has been delegated.
Delegator	Shows you the name of the identity that created the delegation.
Delegation recipient	Shows you the name of the identity to which the responsibility was delegated.
Assignment Method	Shows you what type of delegated responsibility it is. For example, if you delegate responsibility through an identity, the criteria is **Employee manager**.
Delete	Use the buttons to select delegations that you want to delete later using **Actions** > **Delete delegation** (see Deleting my identities' delegations on page 308).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: You can see more information about each action in the details pane.

Attestations – Identity (page description)

To open the **Attestation – Cost center** page go to **Responsibilities** > **My Responsibilities** > **Identities** > select identity > **Attestation**.

On the **Attestation – Identity** page, you can:

- Display all attestation cases linked to this identity (see Displaying attestation cases of my identities on page 309)
- Display details of the objects being attested (see Displaying attestation cases of my identities on page 309)
- Make approval decisions about pending attestation cases (see Approving and denying my identities' attestation cases on page 311)
- Display attestors of pending attestation cases (see Displaying attestors of my identities' pending attestation cases on page 310)
- Send reminders to approvers (see Sending reminders about my identities' pending attestation cases on page 312)

The following tables give you an overview of the various features and content on the **Attestation – Identity** page.

Table 288: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my identities' pending attestation cases on page 310). Then you can send reminder emails to these identities (see Sending reminders about my identities' pending attestation cases on page 312).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my identities' pending attestation cases on page 312).
Approve	Opens the **Pending Attestations – Identity** page (see Pending attestations – Identity (page description) on page 932). Use this button to make approval decisions about attestation cases pending for the identity (see Approving and denying my identities' attestation cases on page 311).

Table 289: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my identities' pending attestation cases on page 310). Then you can send reminder emails to these identities (see Sending reminders about my identities' pending attestation cases on page 312).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying attestation cases of my identities on page 309).

Table 290: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Identity (page description)

To open the **Risk – Identity** page go to **Responsibilities** > **My Responsibilities** > **Identities** > select identity> **Risk**.

On the **Risk – Identity** page, you can:

- Display the identity's calculated risk index (see Displaying my identities' risk indexes on page 314)
- Show how the calculated risk index is put together (see Displaying my identities' risk indexes on page 314)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the various features and content on the **Risk – Identity** page.

Table 291: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying my identities' risk indexes on page 314).

Table 292: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Identity (page description)

To open the **History – Identity** page go to **Responsibilities** > **My Responsibilities** > **Identities** > select identity> **History**.

On the **History – Identity** page, you can see all the identity's changes (see My identities' history on page 315).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect an identity, either on a timeline or in a table (see Displaying my identity history on page 315).

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments (see Displaying the status overview of my identities on page 316). It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

- **Status comparison**: You can select a date and display all the changes made from then until now (see Comparing statuses of my identities on page 317). You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Identity** page.

Table 293: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Deselect the check box if you also want to see properties that have not changed since they were created.

Table 294: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now (see Comparing statuses of my identities on page 317). You can also show what the value of the property was at the selected point in time and what the value is now.

Table 295: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	

Column	Description
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

System entitlements (page description)

To open the **System Entitlements** page go to **Responsibilities** > **My Responsibilities** > **System Entitlements**.

On the **System entitlements** page, you can see all the system entitlements that you manage (see Displaying my system entitlements on page 408).

If you click a system entitlement in the list, a new page opens (see System entitlement overview page (page description) on page 1033), which contains more information and configuration options for the system entitlement.

The following tables give you an overview of the different functions on the **System Entitlements** page.

Table 296: Columns

Column	Description
Name	Shows the system entitlement's name.
Domain/Client	Shows the domain or client that the system entitlement is assigned to.
Requestable	Shows whether the system entitlement can be requested by identities.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

System entitlement overview page (page description)

To open a system entitlement's overview page go to **Responsibilities** > **My Responsibilities** > **System Entitlements** and click a system entitlement.

On the system entitlement's overview page, you can perform various actions on the system entitlement you selected beforehand.

To do this, click on one of the tiles:

Table 297: Tiles

Tile	Description
Overview	Opens the **Overview - System entitlement** page (see Overview – System entitlement (page description) on page 1035). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my system entitlements' overviews on page 408). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - System entitlement** page (see Main data – System entitlement (page description) on page 1035). You perform the following actions: • Display and edit the system entitlement's main data (see Displaying and editing my system entitlements main data on page 409) • Delete Active Directory groups (see Deleting my Active Directory groups on page 410)
Memberships	Opens the **Memberships - System entitlement** page (see Memberships – System entitlement (page description) on page 1037). You select the following actions: • Display identities that are assigned this system entitlement (see Displaying memberships in my system entitlements on page 412) • Request this system entitlement for identities (see Assigning identities to my system entitlements on page 412) • Cancel this system entitlement for identities (see Removing identities from my system entitlements on page 413)
Attestation	Opens the **Attestations – System entitlement** page (see Attestation – System entitlement (page description) on page 1039). You select the following actions:

Tile	Description
	• Display all attestation cases linked to this system entitlement (see Displaying my system entitlements' attestation cases on page 416) • Display details of the objects being attested (see Displaying my system entitlements' attestation cases on page 416) • Make approval decisions about pending attestation cases (see Approving and denying my system entitlements' attestation cases on page 418) • Display attestors of pending attestation cases (see Displaying attestors of my system entitlements' pending attestation cases on page 417) • Send reminders to approvers (see Sending reminders about my system entitlements' pending attestation cases on page 420)
Attestors	Opens the **Attestors – System entitlement** page (see Attestors – System entitlement (page description) on page 1041). You select the following actions: • Display all identities that can be approved through the system entitlement's attestation cases (see Displaying my system entitlements' attestors on page 421). • Specify attestors for the system entitlement (see Specifying attestors for my system entitlements on page 422) • Create new application roles for attestors (see Specifying attestors for my system entitlements on page 422)
Child groups	Open the **Child groups – System entitlement** (see Child groups – System entitlement (page description) on page 1038). You select the following actions: • Display all the system entitlement's child groups (see Display my system entitlements' child groups on page 414) • Assign a child group to the system entitlement (see Assigning child groups to my system entitlements on page 414) • Remove child groups from the system entitlement (see To remove child groups from my system entitlements on page 415)
Owner	Opens the **Owners – System entitlement** page (see Owners – System entitlement (page description) on page 1042). You select the following actions: • Show all the identities that are owners of the system entitlement (see Displaying my system entitlements' product owners on page 423)

Tile	Description
	• Specify owners of the system entitlement (see Specifying product owners for my system entitlements on page 424) • Create new application roles for owners (see Specifying product owners for my system entitlements on page 424)
History	Opens the **History – System entitlement** page (see History – System entitlement (page description) on page 1043). Here you can see all the changes made to the system entitlement (see My system entitlements' history on page 426).
Usage	Opens the **Usage – System entitlement** page (see Usage – System entitlement (page description) on page 1045). Here you can see the roles and organizations that belong to the identities to which this system entitlement is assigned (see Displaying role memberships of my system entitlements' members on page 429).

Overview – System entitlement (page description)

To open the **Overview – System entitlement** page go to **Responsibilities** > **My Responsibilities** > **System Entitlements** > select system entitlement > **Overview**.

On the **Overview – System entitlement** page, you can see all the information relevant to the system entitlement summarized in an overview (see Displaying my system entitlements' overviews on page 408).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – System entitlement (page description)

To open the **Main data – System entitlement** page go to **Responsibilities** > **My Responsibilities** > **System Entitlements** > select system entitlement > **Main data**.

On the **Main data – System entitlement** page, you can:

- Display and edit the system entitlement's main data (see Displaying and editing my system entitlements main data on page 409)
- Delete Active Directory groups (see Deleting my Active Directory groups on page 410)

The following tables give you an overview of the different functions and content on the **Main data – System entitlement** page.

Table 298: Controls

Control	Description
Request modification	NOTE: This button is only available for Active Directory groups.

Control	Description

	Use this button to request the changes to the following properties of the Active Directory group (see Displaying and editing my system entitlements main data on page 409):
	• **Group scope**: Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can specify one of the following group scopes:
	  ◦ **Global group**: Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group’s domain.
	  ◦ **Local**: Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.
	  ◦ **Universal**: Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
	• **Group type**: Specify whether this is an Active Directory security group or an Active Directory distribution group.

Request deletion	NOTE: This button is only available for Active Directory groups. Use this button to request to delete the group (see Deleting my Active Directory groups on page 410).
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 299: System entitlement main data

Property	Description
Name	Enter a full, descriptive name for the system entitlement.
Canonical name	Shows the automatically generated canonical name of the system entitlement.
Distinguished name	Shows the automatically generated distinguished name of the system entitlement.
Display name	Enter a name for displaying the system entitlement in the One Identity Manager tools.
Notes domain	Shows the Notes domain name.

Property	Description
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use a system entitlement until a service item has been assigned to it.
Description	Enter a description for the system entitlement.
Category	Select the category for system entitlement inheritance. User accounts can inherit system entitlements selectively. To do this, system entitlements and user accounts are divided into categories.
Risk index	Use the slider to define the risk index. This value is used to assess the risk of assigning system entitlements to user accounts. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Enable this check box to allow the system entitlement to be requested through the IT Shop. This system entitlement can be requested by your identities through the Web Portal and granted through a defined approval process. The system entitlement can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Enable the check box to allow the system entitlement to be requested through the IT Shop if required. This system entitlement can be requested by your identities through the Web Portal and granted using a defined approval process. The system entitlement may not be assigned directly to hierarchical roles.
IT shop product is inactive	Select the check box if the system entitlement is not used. Only enabled system entitlements can be assigned within One Identity Manager. If a system entitlement is disabled, assignment of the system entitlement is not permitted. However, existing assignments remain intact.

Memberships – System entitlement (page description)

To open the **Memberships – System entitlement** page go to **Responsibilities** > **My Responsibilities** > **System Entitlements** > select system entitlement > **Memberships**.

On the **Memberships – System entitlement** page, you can:

- Display identities that are assigned this system entitlement (see Displaying memberships in my system entitlements on page 412)
- Request this system entitlement for identities (see Assigning identities to my system entitlements on page 412)

- Cancel this system entitlement for identities (see Removing identities from my system entitlements on page 413)

The following tables give you an overview of the different functions and content on the **Memberships – System entitlement** page.

Table 300: Controls

Control	Description
Request memberships	Use this button to request the system entitlement for identities (see Assigning identities to my system entitlements on page 412).
Deleting memberships	Use this button to delete the system entitlement's assignment for selected identities (see Removing identities from my system entitlements on page 413). Select the check box in front of the identities whose membership in the system entitlement you want to delete and click this button.

Table 301: Columns

Column	Description
Identity	Shows you the name of the identity to which the system entitlement is assigned.
Origin	Shows you whether the system entitlement was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Child groups – System entitlement (page description)

To open the **Child groups – System entitlement** page go to **Responsibilities** > **My Responsibilities** > **System Entitlements** > click system entitlement > **Child groups**.

On the **Child groups – System entitlement** page, you can:

- Display all the system entitlement's child groups (see Display my system entitlements' child groups on page 414)
- Assign a child group to the system entitlement (see Assigning child groups to my system entitlements on page 414)
- Remove child groups from the system entitlement (see To remove child groups from my system entitlements on page 415)

The following table gives you an overview of the different features and content on the **Child groups – System entitlement** page.

Table 302: Controls

Control	Description
Remove selected	Use this button to remove selected child groups (see To remove child groups from my system entitlements on page 415). Select the check box in front of the group that you want to remove and click this button.
New child group	Use this button to assign a child group to the system entitlement (see Assigning child groups to my system entitlements on page 414).

Attestation – System entitlement (page description)

To open the **Attestation – System entitlement** page go to **Responsibilities** > **My Responsibilities** > **System Entitlements** > select system entitlement > **Attestation**.

On the **Attestation – System entitlement** page, you can:

- Display all attestation cases linked to this system entitlement (see Displaying my system entitlements' attestation cases on page 416)
- Display details of the objects being attested (see Displaying my system entitlements' attestation cases on page 416)
- Make approval decisions about pending attestation cases (see Approving and denying my system entitlements' attestation cases on page 418)
- Display attestors of pending attestation cases (see Displaying attestors of my system entitlements' pending attestation cases on page 417)
- Send reminders to approvers (see Sending reminders about my system entitlements' pending attestation cases on page 420)

The following tables give you an overview of the various features and content on the **Attestation – System entitlement** page.

Table 303: Controls

Control	Description
View approvers for pending	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my

Control	Description
cases	system entitlements' pending attestation cases on page 417). Then you can send reminder emails to these identities (see Sending reminders about my system entitlements' pending attestation cases on page 420).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my system entitlements' pending attestation cases on page 420).
Approve	Opens the **Pending Attestations – System entitlements** page (see Pending attestations – System entitlement (page description) on page 943). Use this button to make approval decisions about attestation cases pending for the system entitlement (see Approving and denying my system entitlements' attestation cases on page 418).

Table 304: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my system entitlements' pending attestation cases on page 417). Then you can send reminder emails to these identities (see Sending reminders about my system entitlements' pending attestation cases on page 420).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my system entitlements' attestation cases on page 416).

Table 305: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was

Column	Description
	granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestors – System entitlement (page description)

To open the **Attestors – System entitlement** page go to **Responsibilities** > **My Responsibilities** > **System Entitlements** > select system entitlement > **Attestors**.

On the **Attestors – System entitlement** page, you can:

- Display all identities that can be approved through the system entitlement's attestation cases (see Displaying my system entitlements' attestors on page 421).
- Specify attestors for the system entitlement (see Specifying attestors for my system entitlements on page 422)
- Create new application roles for attestors (see Specifying attestors for my system entitlements on page 422)

The following tables give you an overview of the various features and content on the **Attestor – System entitlement** page.

Table 306: Controls

Control	Description
Attestors	Click **Assign**/**Change** and select an application role whose members can approve the system entitlement's attestation cases (see Specifying attestors for my system entitlements on page 422). To save the changes, click **Save**.
New	Use this button to create a new application role (see Specifying attestors for my system entitlements on page 422). Then you can assign identities to the new application role that can approve the system entitlement's attestation cases. To save the changes, click **Save**.
Save	Use this button to save all the changes you have made.

Table 307: Columns

Column	Description
Name	Shows you the name of the identity that you can assign to the application role.
Primary department	Shows you which department is assigned as primary to the identity.
Identity	Shows you whether this is a main or a sub identity.

Owners – System entitlement (page description)

To open the **Owners – System entitlement** page go to **Responsibilities** > **My Responsibilities** > **System Entitlements** > select system entitlement > **Owners**.

On the **Owners – System entitlement** page, you can:

- Show all the identities that are owners of the system entitlement (see Displaying my system entitlements' product owners on page 423)
- Specify owners of the system entitlement (see Specifying product owners for my system entitlements on page 424)
- Create new application roles for owners (see Specifying product owners for my system entitlements on page 424)

The following tables give you an overview of the different features and content on the **Owners – System entitlement** page.

Table 308: Controls

Control	Description
Product owners	Click **Assign**/**Change** and select an application role whose members will be owners of the system entitlement (see Specifying product owners for my system entitlements on page 424). To save the changes, click **Save**.
New	Use this button to create a new application role (see Specifying product owners for my system entitlements on page 424). Then you can assign identities to the new application role to be the owners of the system entitlement. To save the changes, click **Save**.
Move ownership	Use this button to create a new application role and, at the same time, transfer all the currently assigned owners to it (see Specifying product owners for my system entitlements on page 424). To save the changes, click **Save**.
Save	Use this button to save all the changes you have made.

Table 309: Columns

Column	Description
Name	Shows you the name of the identity that you can assign to the application role.
Primary department	Shows the department that the identity is primarily assigned to.
Identity	Shows you whether this is a main or a sub identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

History – System entitlement (page description)

Open the **History – System entitlement** page by navigating through **Responsibilities** > **My Responsibilities** > **System Entitlements** > select system entitlement > **History**.

On the **History – System entitlements** page, you can show all the system entitlement's changes (see My system entitlements' history on page 426).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table (see Displaying my system entitlements' history on page 426).

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.
- **Status overview**: Shows an overview of all assignments (see Displaying the status my system entitlements' overview on page 427). It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now (see Comparing statuses of my system entitlements on page 428). You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – System entitlement** page.

Table 310: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For

Control	Description
	example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Deselect the check box if you also want to see properties that have not changed since they were created.

Table 311: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now (see Comparing statuses of my system entitlements on page 428). You can also show what the value of the property was at the selected point in time and what the value is now.

Table 312: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.

Column	Description
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – System entitlement (page description)

To open the **Usage – System entitlement** page go to **Responsibilities** > **My Responsibilities** > **System Entitlements** > select system entitlement > **Usage**.

On the **Usage – System entitlement** page, you can see the roles and organizations that belong to the identities to which this system entitlement is assigned (see Displaying role memberships of my system entitlements' members on page 429).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the various features on the **Usage – System entitlement** page.

Table 313: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to see (see Displaying role memberships of my system entitlements' members on page 429).
More information	Use this button to show the legend that explains the content of the overview (see Displaying role memberships of my system entitlements' members on page 429).

Business roles (page description)

To open the **Business Roles** page go to **Responsibilities** > **My Responsibilities** > **Business Roles**.

On the **Business Roles** page, you can:

- View all the business roles that you manage (see Displaying my business roles on page 270)
- Create new business roles (see Creating your own business roles on page 271)
- Restore deleted business roles (see Restoring deleted my business roles on page 271)

If you click a business role in the list, a new page opens (see Business role overview page (page description) on page 1047), which contains more information and configuration options for the business role.

The following tables give you an overview of the different functions and content on the **Business roles** page.

Table 314: Controls

Control	Description
New business roles	Opens the **Create a new business role** page (see Creating new business roles (page description) on page 1046). Use this button to add a new business role to the system (see Creating your own business roles on page 271).
To restore a deleted role	Use this button to restore a deleted business role (see Restoring deleted my business roles on page 271).

Table 315: Columns

Column	Description
Name	Shows the business role's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Creating new business roles (page description)

To open the **Create a new business role** page go to **Responsibilities** > **My Responsibilities** > **Business Roles** > **New business role**.

On the **Create new business role** page, you can create a new business role for which you are responsible. Do this by entering the new business role's main data (see Creating your own business roles on page 271).

Enter the following main data.

Table 316: Business role main data

Property	Description
Business role	Enter a full, descriptive name for the business role.
Short name	Enter a short name for the business role.
Internal name	Enter a company internal name for the business role.
Description	Enter a description for the business role.
Role class	When you create the business role: Select the role class of the business role. To differentiate between different business roles, define company specific role classes. Role classes are used to specify which company resource assignments are possible through roles in a role class.
Parent business role	Click **Assign/Change** and select a business role to be the parent business role for organizing the business role hierarchically. If you want the business role at the root of a business role hierarchy, leave the field empty.
Role type	Select the role type of the business role. Role types are mainly used to regulate approval policy inheritance.
Role approver	Click **Assign/Change** and select an application role. Members of the selected application role can approve requests for members of the business role.
Role approver (IT)	Click **Assign/Change** and select an application role. Members of the selected application role can approve requests for members of the business role.
Manager	Click **Assign/Change** and select the manager responsible for the business role.
2nd Manager	Click **Assign/Change** and select an identity to act as a deputy to the business role's manager.
Employees do not inherit	Select this check box if you want to temporarily prevent identities from inheriting this business role.
Comment	Enter a comment for the business role.

Business role overview page (page description)

To open a business role's overview page go to **Responsibilities** > **My Responsibilities** > **Business Roles** and click a business role.

On the business role's overview page, you can perform various actions on the business role you selected beforehand.

To do this, click on one of the tiles:

Table 317: Tiles

Tile	Description
Overview	Opens the **Overview - Business role** page (see Overview – Business role (page description) on page 1050). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my business roles' overviews on page 274). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Business role** page (see Main data – Business role (page description) on page 1050). Here you can see and edit the business role's main data (see Displaying and editing my business roles' main data on page 275).
Memberships	Opens the **Memberships - Business role** page (see Memberships – Business role (page description) on page 1051). You select the following actions: • Display identities that are assigned this business role (see Displaying my business roles' memberships on page 275) • Request the business role for identities (see Assigning identities to my business roles on page 276) • Cancel this business role for identities (see Removing identities from my business roles on page 277)
Permissions	Opens the **Entitlements – Business role** page (see Entitlements – Business role (page description) on page 1052). You select the following actions: • Display entitlements assigned to the business role (see Displaying my business roles' entitlements on page 278) • Add new entitlements (see Adding my business roles' entitlements on page 278) • Delete business role entitlements (see Deleting my business roles' entitlements on page 279)
Compliance	Opens the **Compliance – Business role** page (see Compliance – Business role (page description) on page 1053). Here you can see rule violations that were caused by this business role (see Displaying my business roles' rule violations on page 281).
Attestation	Opens the **Attestation – Business role** page (see Attestation – Business role (page description) on page 1054). You select the following actions:

Tile	Description
	• Display all attestation cases linked to this business role (see Displaying my business roles' attestation cases on page 283) • Display details of the objects being attested (see Displaying my business roles' attestation cases on page 283) • Make approval decisions about pending attestation cases (see Approving and denying my business roles' attestation cases on page 286) • Display attestors of pending attestation cases (see Displaying attestors of my business roles' pending attestation cases on page 285) • Send reminders to approvers (see Sending reminders about my business roles' pending attestation cases on page 287)
Risk	Opens the **Risk – Business role** page (see Risk – Business role (page description) on page 1056). Here you can see the business role's risk index (see Displaying my business roles' risk indexes on page 289). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – Business role** page (see History – Business role (page description) on page 1057). Here you can see all the changes made to the business role and reset the business role to a historical state (see My business roles' history on page 289).
Usage	Opens the **Usage – Business role** page (see Usage – Business role (page description) on page 1059). Here you can see which roles and organizations belong to members of the business role (see Displaying role memberships of my business roles' members on page 294).
Compliance reports	Opens the **Compliance report – Business role** page (see Compliance reports – Business role (page description) on page 1059). You select the following actions: • Display the business role's policy violations (see Displaying my business roles' policy violations on page 281) • Display rule violations of identities that the business role is assigned to (see Displaying rule violations of my business roles' members on page 282) • Display risk indexes and entitlements of identities that the business role is assigned to (see Displaying risk indexes and entitlements of my business roles' members on page 282)

Tile	Description
Split	You can copy or move memberships and entitlements from the business role to a new role (department, business role, cost center, location) (see Copying/splitting my business roles on page 294).
Compare and merge	You can copy or move properties of the business role to another role (department, business role, cost center, location) for which you are responsible, compare them and then select the properties you require and merge them (see Comparing and merging my business roles on page 296).
Redo	Here you can restore a deleted business role that was under this business role (see Restoring deleted my business roles on page 271).

Overview – Business role (page description)

To open the **Overview – Business role** page go to **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role > **Overview**.

On the **Overview - Business role** page, you can see all the information relevant to the business role summarized in an overview (see Displaying my business roles' overviews on page 274).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Business role (page description)

To open the **Main data – Business role** page go to **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role > **Main data**.

On the **Main data - Business role** page, you can show and edit the business role's main data (see Displaying and editing my business roles' main data on page 275).

The following tables give you an overview of the different functions and content on the **Main data – Business role** page.

Table 318: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 319: Business role main data

Property	Description
Business role	Enter a full, descriptive name for the business role.

Property	Description
Short name	Enter a short name for the business role.
Internal name	Enter a company internal name for the business role.
Description	Enter a description for the business role.
Role class	When you create the business role: Select the role class of the business role. To differentiate between different business roles, define company specific role classes. Role classes are used to specify which company resource assignments are possible through roles in a role class.
Parent business role	Click **Assign/Change** and select a business role to be the parent business role for organizing the business role hierarchically. If you want the business role at the root of a business role hierarchy, leave the field empty.
Role type	Select the role type of the business role. Role types are mainly used to regulate approval policy inheritance.
Role approver	Click **Assign/Change** and select an application role. Members of the selected application role can approve requests for members of the business role.
Role approver (IT)	Click **Assign/Change** and select an application role. Members of the selected application role can approve requests for members of the business role.
Manager	Click **Assign/Change** and select the manager responsible for the business role.
2nd Manager	Click **Assign/Change** and select an identity to act as a deputy to the business role's manager.
Employees do not inherit	Select this check box if you want to temporarily prevent identities from inheriting this business role.
Comment	Enter a comment for the business role.

Memberships – Business role (page description)

To open the **Memberships – Business role** page go to **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role > **Memberships**.

On the **Memberships - Business role** page, you can:

- Display identities that are assigned this business role (see Displaying my business roles' memberships on page 275)

- Request the business role for identities (see Assigning identities to my business roles on page 276)
- Cancel this business role for identities (see Removing identities from my business roles on page 277)

The following tables give you an overview of the different functions and content on the **Memberships – Business role** page.

Table 320: Controls

Control	Description
Request memberships	Use this button to request the business role for identities (see Assigning identities to my business roles on page 276).
Deleting memberships	Use this button to delete the resource's assignment for selected identities (see Removing identities from my business roles on page 277). Select the check box in front of the identities whose membership in the system entitlement you want to delete and click this button.

Table 321: Columns

Column	Description
Identity	Shows you the name of the identity to which the business role is assigned.
Origin	Shows you whether the business role was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Business role (page description)

To open the **Entitlements – Business role** page go to **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role > **Entitlements**.

On the **Entitlements – Business role** page, you can:

- Display entitlements assigned to the business role (see Displaying my business roles' entitlements on page 278)
- Add new entitlements (see Adding my business roles' entitlements on page 278)
- Delete business role entitlements (see Deleting my business roles' entitlements on page 279)

The following tables give you an overview of the different functions and content on the **Entitlements – Business role** page.

Table 322: Controls

Control	Description
New	Use this button to add a new entitlement to the business role (see Adding my business roles' entitlements on page 278). Identities that this business role is assigned to, automatically obtain membership in the object assigned here.
Remove	Use this button to delete selected entitlements (see Deleting my business roles' entitlements on page 279). To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 323: Columns

Column	Description
Entitlement	Shows the entitlement's name.
Origin	Shows how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Business role (page description)

To open the **Compliance – Business role** page go to **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role > **Compliance**.

On the **Compliance – Business role** page, you can see the rule violations caused by the business role (see Displaying my business roles' rule violations on page 281).

The following table gives an overview of the content of the **Compliance – Business role** page.

Table 324: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Business role (page description)

To open the **Attestation – Business role** page go to **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role > **Attestation**.

On the **Attestation – Business role** page, you can:

- Display all attestation cases linked to this business role (see Displaying my business roles' attestation cases on page 283)
- Display details of the objects being attested (see Displaying my business roles' attestation cases on page 283)
- Make approval decisions about pending attestation cases (see Approving and denying my business roles' attestation cases on page 286)
- Display attestors of pending attestation cases (see Displaying attestors of my business roles' pending attestation cases on page 285)
- Send reminders to approvers (see Sending reminders about my business roles' pending attestation cases on page 287)

The following tables give you an overview of the various features and content on the **Attestation – Business role** page.

Table 325: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my business roles' pending attestation cases on page 285). Then you can send reminder emails to these identities (see Sending reminders about my business roles' pending attestation cases on page 287).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my business roles' pending attestation cases on page 287).
Approve	Opens the **Pending Attestations – Business roles** page (see Pending attestations – Business role (page description) on page 920). Use this button to make approval decisions about attestation cases pending for the business role (see Approving and denying my business roles' attestation cases on page 286).

Table 326: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my business roles' pending attestation cases on page 285). Then you can send reminder emails to these identities (see Sending reminders about my business roles' pending attestation cases on page 287).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my business roles' attestation cases on page 283).

Table 327: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane,

Column	Description
	on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Business role (page description)

To open the **Risk – Business role** page go to **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role > **Risk**.

On the **Risk – Business role** page, you can:

- Display the business role's calculated risk index (see Displaying my business roles' risk indexes on page 289)
- Show how the calculated risk index is put together (see Displaying my business roles' risk indexes on page 289)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – Business role** page.

Table 328: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying my business roles' risk indexes on page 289).

Table 329: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment.

Column	Description
	• At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Business role (page description)

Open the **History – Business role** page by navigating through **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role > **History**.

On the **History – Business role** page, you can show all the business role's changes and reset the business role to a previous state (see My business roles' history on page 289).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a business role, either on a timeline or in a table (see Displaying my business roles' history on page 290).

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments (see Displaying the status overview of my business roles on page 291). It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now (see Comparing statuses of my business roles on page 291). You can also show what the value of the property was at the selected point in time and what the value is now. You can roll back the business role to this historical state (see Roll back my business roles to historical state on page 292).

The following tables give you an overview of the different functions and content on the **History – Business role** page.

Table 330: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.

Control	Description
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Deselect the check box if you also want to see properties that have not changed since they were created.
Roll back changes	Use this button to roll back the business role to a previous state (see Roll back my business roles to historical state on page 292).

Table 331: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now (see Comparing statuses of my business roles on page 291). You can also show what the value of the property was at the selected point in time and what the value is now.

Table 332: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.

Column	Description
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Business role (page description)

To open the **Usage – Business role** page go to **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role > **Usage**.

On the **Usage – Business role** page, you can see the roles and organizations that belong to the identities to which this business role is assigned (see Displaying role memberships of my business roles' members on page 294).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the various features on the **Usage – Business role** page.

Table 333: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to see (see Displaying role memberships of my business roles' members on page 294).
More information	Use this button to show the legend that explains the content of the overview (see Displaying role memberships of my business roles' members on page 294).

Compliance reports – Business role (page description)

Open the **Compliance reports – Business role** page by navigating through **Responsibilities** > **My Responsibilities** > **Business Roles** > select business role >

Compliance reports.

On the **Compliance Reports - Business role** page you can:

- Display the business role's policy violations (see Displaying my business roles' policy violations on page 281)
- Display rule violations of identities that the business role is assigned to (see Displaying rule violations of my business roles' members on page 282)
- Display risk indexes and entitlements of identities that the business role is assigned to (see Displaying risk indexes and entitlements of my business roles' members on page 282)

The information is divided into three parts:

- **Policy violations**: Displays all the current policy violations caused by the application role.
- **Compliance rule violations**: Shows you the current rule violations of the identities to which the business role is assigned.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and authorizations**: Displays all identities to which the business role is assigned. Additionally, the number of assigned entitlements and the risk index of these identities are displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – Business role** page.

Table 334: Columns

Column	Description
Policy violations	
Violating object	Shows you which object caused the rule violation.
Policy	Shows you the policy that was violated.
Status	Shows you the status of the rule policy.
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows you the violated rule.
Approval state	Shows you how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied.

Column	Description
	Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.
Identities: Risk index and entitlements	
Identities	Shows you the identity to which this business role is assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

System roles (page description)

To open the **System Roles** page go to **Responsibilities** > **My Responsibilities** > **System Roles**.

On the **System Roles** page, you can:

- View all the system roles that you manage (see Displaying my system roles on page 430)
- Create new system roles (see Creating your own system roles on page 431)

If you click a system role in the list, a new page opens (see System role overview page (page description) on page 1063), which contains more information and configuration options for the system role.

The following tables give you an overview of the different functions and content on the **System Roles** page.

Table 335: Controls

Control	Description
New system role	Opens the **New system role** page (see New system role (page description) on page 1062). Use this button to add a new system role to the system (see Creating your own system roles on page 431).

Table 336: Columns

Column	Description
Name	Shows the system role's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

New system role (page description)

To open the **New system Roles** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > **New system role**.

On the **New System Role** page, you can create a new system role for which you are responsible. Do this by entering the new system role's main data (see Creating your own system roles on page 431).

Enter the following main data.

Table 337: System role main data

Property	Description
System role	Enter a full, descriptive name for the system role.
Display name	Enter a name for displaying the system role in the One Identity Manager tools.
Internal product name	Enter a company internal name for the system role.
System role type	Select the role type of the system role. The system role type specifies which type of company resources make up the system role.
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use a system role until a service item has been assigned to it.
System role manager	Click **Change** and select the identity responsible for the system role. This identity can edit the system role's main data and be used as an attestor for system role properties. If the system role can be requested in the IT Shop, the manager will automatically be a member of the application role for product owners assigned the service item.
Comment	Enter a comment for the system role.
IT shop	Select the check box if the system role can also be requested through the IT Shop. This system role can be requested by identities through the Web Portal and the request granted by a defined approval process. The system role can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One*

Property	Description
	Identity Manager IT Shop Administration Guide.
Only use in IT Shop	Select the check box if the system role can only be requested through the IT Shop. This system role can be requested by identities through the Web Portal and the request granted by a defined approval process. The system role may not be assigned directly to hierarchical roles.

System role overview page (page description)

To open a system role's overview page go to **Responsibilities** > **My Responsibilities** > **System Roles** and click a system role.

On the system role's overview page, you can perform various actions on the system role you selected beforehand.

To do this, click on one of the tiles:

Table 338: Tiles

Tile	Description
Overview	Opens the **Overview - System role** page (see Overview – System role (page description) on page 1065). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my system roles' overviews on page 431). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - System role** page (see Main data – System role (page description) on page 1065). Here you can see and edit the system role's main data (see Displaying and editing my system roles' main data on page 432).
Memberships	Opens the **Memberships - System role** page (see Memberships – System role (page description) on page 1067). You select the following actions: • Display identities that are assigned this system role (see Displaying memberships in my system roles on page 432) • Request the system role for identities (see Assigning identities to my system roles on page 433) • Cancel this system role for identities (see Removing identities from my system roles on page 434)
Permissions	Opens the **Entitlements – System role** page (see Entitlements – System role (page description) on page 1066). You select the following actions:

Tile	Description
	• Display entitlements assigned to the system role (see Displaying my system roles' entitlements on page 435) • Add new entitlements to the system role (see Adding my system roles' entitlements on page 435) • Delete system role entitlements (see Deleting my system roles' entitlements on page 436)
Compliance	Opens the **Compliance – System role** page (see Compliance – System role (page description) on page 1068). Here you can see rule violations that were caused by this system role (see Displaying my system roles' rule violations on page 437).
Attestation	Opens the **Attestation – System role** page (see Attestation – System role (page description) on page 1069). You select the following actions: • Display all attestation cases linked to this system role (see Displaying my system roles' attestation cases on page 440) • Display details of the objects being attested (see Displaying my system roles' attestation cases on page 440) • Make approval decisions about pending attestation cases (see Approving and denying my system roles' attestation cases on page 443) • Display attestors of pending attestation cases (see Displaying attestors of my system roles' pending attestation cases on page 442) • Send reminders to approvers (see Sending reminders about my system roles' pending attestation cases on page 444)
Risk	Opens the **Risk – System role** page (see Risk – System role (page description) on page 1071). Here you can see the system role's risk index (see Displaying my system roles' risk indexes on page 446). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – System role** page (see History – System role (page description) on page 1072). Here you can see all the changes made to the system role (see My system roles' history on page 446).
Usage	Opens the **Usage – System role** page (see Usage – System role (page description) on page 1074). Here you can see which roles and organizations belong to members of the system role (see Displaying role memberships of my system roles'

Tile	Description
	members on page 449).
Compliance reports	Opens the **Compliance report – System role** page (see Compliance reports – system role (page description) on page 1074). You select the following actions: • Display the system role's policy violations (see Displaying my system roles' policy violations on page 438) • Display rule violations of identities that the system role is assigned to (see Displaying rule violations of my system roles' members on page 438) • Display risk indexes and entitlements of identities that the system role is assigned to (see Displaying risk indexes and entitlements of my system roles' members on page 439)

Overview – System role (page description)

To open the **Overview – System role** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **Overview**.

On the **Overview - System role** page, you can see all the information relevant to the system role in summarized in an overview (see Displaying my system roles' overviews on page 431).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – System role (page description)

To open the **Main data – System role** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **Main data**.

On the **Main data - System role** page, you can show and edit the system role's main data (see Displaying and editing my system roles' main data on page 432).

The following tables give you an overview of the different functions and content on the **Main data – System role** page.

Table 339: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 340: System role main data

Property	Description
System role	Enter a full, descriptive name for the system role.
Display name	Enter a name for displaying the system role in the One Identity Manager tools.
Internal product name	Enter a company internal name for the system role.
System role type	Select the role type of the system role. The system role type specifies which type of company resources make up the system role.
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use a system role until a service item has been assigned to it.
System role manager	Click **Change** and select the identity responsible for the system role. This identity can edit the system role's main data and be used as an attestor for system role properties. If the system role can be requested in the IT Shop, the manager will automatically be a member of the application role for product owners assigned the service item.
Comment	Enter a comment for the system role.
IT shop	Select the check box if the system role can also be requested through the IT Shop. This system role can be requested by identities through the Web Portal and the request granted by a defined approval process. The system role can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the system role can only be requested through the IT Shop. This system role can be requested by identities through the Web Portal and the request granted by a defined approval process. The system role may not be assigned directly to hierarchical roles.

Entitlements – System role (page description)

To open the **Entitlements – System role** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **Entitlements**.

On the **Entitlements – System role** page, you can:

- Display entitlements assigned to the system role (see Displaying my system roles' entitlements on page 435)
- Add new entitlements to the system role (see Adding my system roles' entitlements on page 435)
- Delete system role entitlements (see Deleting my system roles' entitlements on page 436)

The following tables give you an overview of the different functions and content on the **Entitlements – System role** page.

Table 341: Controls

Control	Description
New	Use this button to add a new entitlement to the system role (see Adding my system roles' entitlements on page 435). Identities that this system role is assigned to, automatically obtain membership in the object assigned here.
Remove	Use this button to delete selected entitlements . To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 342: Columns

Column	Description
Entitlement	Shows the entitlement's name.
Origin	Shows how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Memberships – System role (page description)

To open the **Memberships – System role** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **Memberships**.

On the **Memberships - System role** page, you can:

- Display identities that are assigned this system role (see Displaying memberships in my system roles on page 432)
- Request the system role for identities (see Assigning identities to my system roles on page 433)
- Cancel this system role for identities (see Removing identities from my system roles on page 434)

The following tables give you an overview of the different functions and content on the **Memberships – System role** page.

Table 343: Controls

Control	Description
Request memberships	Use this button to request the system role for identities (see Assigning identities to my system roles on page 433).
Deleting memberships	Use this button to delete the system role's assignment for selected identities (see Removing identities from my system roles on page 434). Select the check box in front of the identities whose membership in the system role you want to delete and click this button.

Table 344: Columns

Column	Description
Identity	Shows you the name of the identity to which the system role is assigned.
Origin	Shows you whether the system role was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – System role (page description)

To open the **Compliance – System role** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **Compliance**.

On the **Compliance – System role** page, you can see the rule violations caused by the system role. (see Displaying my system roles' rule violations on page 437).

The following table gives an overview of the content of the **Compliance – System role** page.

Table 345: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – System role (page description)

To open the **Attestation – System role** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **Attestation**.

On the **Attestation – System role** page, you can:

- Display all attestation cases linked to this system role (see Displaying my system roles' attestation cases on page 440)
- Display details of the objects being attested (see Displaying my system roles' attestation cases on page 440)
- Make approval decisions about pending attestation cases (see Approving and denying my system roles' attestation cases on page 443)
- Display attestors of pending attestation cases (see Displaying attestors of my system roles' pending attestation cases on page 442)
- Send reminders to approvers (see Sending reminders about my system roles' pending attestation cases on page 444)

The following tables give you an overview of the various features and content on the **Attestation – System role** page.

Table 346: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my system roles' pending attestation cases on page 442). Then you can send reminder emails to these identities (see Sending reminders about my system roles' pending attestation cases on page 444).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my system roles' pending attestation cases on page 444).
Approve	Opens the **Pending Attestations – System roles** page (see Pending attestations – System role (page description) on page 912). Use this button to make approval decisions about attestation cases pending for the system role (see Approving and denying my system roles' attestation cases on page 443).

Table 347: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my system roles' pending attestation cases on page 442). Then you can send reminder emails to these identities (see Sending reminders about my system roles' pending attestation cases on page 444).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my system roles' attestation cases on page 440).

Table 348: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane,

Column	Description
	on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – System role (page description)

To open the **Risk – System role** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **Risk**.

On the **Risk – System role** page, you can:

- Display the system role's calculated risk index (see Displaying my system roles' risk indexes on page 446)
- Show how the calculated risk index is put together (see Displaying my system roles' risk indexes on page 446)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – System role** page.

Table 349: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying my system roles' risk indexes on page 446).

Table 350: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment.

Column	Description
	• At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – System role (page description)

Open the **History – System role** page by navigating through **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **History**.

On the **History – System role** page, you can show all the system role's changes (see My system roles' history on page 446).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system role, either on a timeline or in a table (see Displaying my system roles' history on page 447).

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments (see Displaying the status overview of my system roles on page 448). It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now (see Comparing statuses of my system roles on page 448). You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – System role** page.

Table 351: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table	Use this button to display the changes in table form.

Control	Description
view	
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Deselect the check box if you also want to see properties that have not changed since they were created.

Table 352: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now (see Comparing statuses of my system roles on page 448). You can also show what the value of the property was at the selected point in time and what the value is now.

Table 353: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.

Column	Description
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – System role (page description)

To open the **Usage – System role** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **Usage**.

On the **Usage – System role** page, you can see the roles and organizations that belong to the identities to which this system role is assigned (see Displaying role memberships of my system roles' members on page 449).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the various features on the **Usage – System role** page.

Table 354: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to see (see Displaying role memberships of my system roles' members on page 449).
More information	Use this button to show the legend that explains the content of the overview (see Displaying role memberships of my system roles' members on page 449).

Compliance reports – system role (page description)

Open the **Compliance reports – System role** page by navigating through **Responsibilities** > **My Responsibilities** > **System Roles** > select system role > **Compliance reports**.

On the **Compliance Reports - System role** page you can:

- Display the system role's policy violations (see Displaying my system roles' policy violations on page 438)
- Display rule violations of identities that the system role is assigned to (see Displaying rule violations of my system roles' members on page 438)
- Display risk indexes and entitlements of identities that the system role is assigned to (see Displaying risk indexes and entitlements of my system roles' members on page 439)

The information is divided into three parts:

- **Policy violations**: Shows you all the current policy violations caused by the system role.
- **Compliance rule violations**: Shows you the current rule violations of the identities to which the system role is assigned.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and authorizations**: Displays all identities to which the system role is assigned. Additionally, the number of assigned entitlements and the risk index of these identities are displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – System role** page.

Table 355: Columns

Column	Description
Policy violations	
Violating object	Shows you which object caused the rule violation.
Policy	Shows you the policy that was violated.
Status	Shows you the status of the rule policy.
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows you the violated rule.
Approval state	Shows you how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance –

Column	Description
	Governance Administration on page 209.
Identities: Risk index and entitlements	
Identities	Shows you the identity to which this system role is assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Departments (page description)

To open the **Departments** page go to **Responsibilities** > **My Responsibilities** > **Departments**.

On the **Departments** page, you can:

- View all the departments that you manage (see Displaying my departments on page 221)
- Restore deleted departments (see Restoring my deleted departments on page 221)

If you click a department in the list, a new page opens (see Department overview page (page description) on page 1077), which contains more information and configuration options for the department.

The following tables give you an overview of the different functions and content on the **Departments** page.

Table 356: Controls

Control	Description
To restore a deleted role	Use this button to restore a deleted department (see Restoring my deleted departments on page 221).

Table 357: Columns

Column	Description
Name	Shows the department's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Department overview page (page description)

To open a department's overview page go to **Responsibilities** > **My Responsibilities** > **Departments** and click a department.

On the department's overview page, you can perform various actions on the department you selected beforehand.

To do this, click on one of the tiles:

Table 358: Tiles

Tile	Description
Overview	Opens the **Overview - Department** page (see Overview – Department (page description) on page 1079) Here you can see all the relevant information about departments summarized in an overview. (see Displaying my department overviews on page 222). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Department** page (see Main data – Department (page description) on page 1079). Here you can see and edit the department's main data (see Displaying and editing my department main data on page 223).
Memberships	Opens the **Memberships - Department** page (see Memberships – Department (page description) on page 1080). You select the following actions: • Display identities that are assigned this department (see Displaying memberships in my departments on page 224) • Assign identities to the department (see Assigning identities to my departments on page 224) • Remove identities from the department (see Removing identities from my departments on page 225)
Permissions	Opens the **Entitlements – Department** page (see Entitlements – Department (page description) on page 1081) You select the following actions: • Display entitlements assigned to this department (see Displaying my department entitlements on page 226) • Add new entitlements to the department (see Adding my department entitlements on page 226) • Delete department entitlements (see Deleting my department entitlements on page 227)
Compliance	Opens the **Compliance – Department** page (see Compliance –

Tile	Description
	Department (page description) on page 1082). Here you can see rule violations that were caused by this department (see Displaying my departments' rule violations on page 229).
Attestation	Opens the **Attestations – Department** page (see Attestation – Department (page description) on page 1083). You select the following actions: • Display all attestation cases linked to this department (see Displaying my department attestation cases on page 231) • Display details of the objects being attested (see Displaying my department attestation cases on page 231) • Make approval decisions about pending attestation cases (see Approving and denying my department attestation cases on page 234) • Display attestors of pending attestation cases (see Displaying attestors of my department pending attestation cases on page 233) • Send reminders to approvers (see Sending reminders about my department pending attestation cases on page 235)
Risk	Opens the **Risk – Department** page (see Risk – Department (page description) on page 1085) Here you can see the department's risk index (see Displaying my department risk indexes on page 236). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – Department** page (see History – Department (page description) on page 1086) Here you can see all the changes made to the department (see My departments' history on page 237).
Usage	Opens the **Usage – Department** page (see Usage – Department (page description) on page 1088) Here you can see which roles and organizations belong to members of the department (see Displaying role memberships of my department members on page 240)
Compliance reports	Opens the **Compliance report – Department** page (see Compliance reports – Department (page description) on page 1088). You select the following actions: • Display the department's policy violations (see Displaying my department policy violations on page 229)

Tile	Description
	• Display rule violations of identities that the department is assigned to (see Displaying rule violations of my department members on page 230) • Display risk indexes and entitlements of identities that the department is assigned to (see Displaying risk indexes and entitlements of my department members on page 230)
Split	You can copy or move memberships and entitlements from the department to a new role (department, business role, cost center, location) (see Copying/splitting my departments on page 241).
Compare and merge	You can copy or move properties of the department to another role (department, business role, cost center, location) for which you are responsible, compare them and then select the properties you require and merge them (see Comparing and merging my departments on page 242).
Redo	Here you can restore a deleted department that was under this department (see Restoring my deleted departments on page 221).
Statistics	Here you can see various statistics about the department (see Displaying my department statistics on page 244).

Overview – Department (page description)

To open the **Overview – Department** page go to **Responsibilities** > **My Responsibilities** > **Departments** > select department > **Overview**.

On the **Overview – Department** page, you can see all the information relevant to the department summarized in an overview (see Displaying my department overviews on page 222).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Department (page description)

To open the **Main data – Department** page go to **Responsibilities** > **My Responsibilities** > **Departments** > select department > **Main data**.

On the **Main data - Department** page, you can show and edit the department's main data (see Displaying and editing my department main data on page 223).

The following tables give you an overview of the different functions and content on the **Main data – Department** page.

Table 359: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 360: Department main data

Property	Description
Department	Enter a full, descriptive name for the department.
Short name	Enter a short name for the department.
Object ID	Enter a unique object ID for the department. For example, the object ID is required in SAP systems for assigning identities to departments.
Parent department	Click **Assign**/**Change** and select a department to be the parent department for organizing the department hierarchically. If you want the department at the root of a department hierarchy, leave the field empty.
Manager	Click **Assign**/**Change** and select the manager responsible for the department.
2nd Manager	Click **Assign**/**Change** and select an identity to act as a deputy to the department's manager.
Location	Click **Assign**/**Change** and select the location the cost center is primarily assigned to.
Attestors	Click **Assign**/**Change** and select a cost center. Members of the selected application role can approve attestation cases for the department.
Cost center	Click **Assign**/**Change** and select the location the department is primarily assigned to.
Role approver	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the department.
Role approver (IT)	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the department.
Description	Enter a description for the department.

Memberships – Department (page description)

To open the **Memberships – Department** page go to **Responsibilities** > **My Responsibilities** > **Departments** > select department > **Memberships**.

On the **Memberships - Department** page, you can:

- Display identities that are assigned this department (see Displaying memberships in my departments on page 224)
- Assign identities to the department (see Assigning identities to my departments on page 224)

- Remove identities from the department (see Removing identities from my departments on page 225)

The following tables give you an overview of the different functions and content on the **Memberships – Department** page.

Table 361: Controls

Control	Description
Request memberships	Use this button to request membership in the department for identities (see Assigning identities to my departments on page 224).
Deleting memberships	Use this button to remove selected identities from the department (see Removing identities from my departments on page 225). Select the check boxes in front of the identities you want to remove from the department and click this button.

Table 362: Columns

Column	Description
Identity	Shows you the name of the identity assigned to the department.
Origin	Shows you whether the department of the identity was assigned directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Department (page description)

To open the **Entitlements – Department** page go to **Responsibilities** > **My Responsibilities** > **Departments** > select department > **Entitlements**.

On the **Entitlements – Department** page, you can:

- Display entitlements assigned to this department (see Displaying my department entitlements on page 226)
- Add new entitlements to the department (see Adding my department entitlements on page 226)
- Delete department entitlements (see Deleting my department entitlements on page 227)

The following tables give you an overview of the different functions and content on the **Entitlements – Department** page.

Table 363: Controls

Control	Description
New	Use this button to add a new entitlement to the department (see Adding my department entitlements on page 226). Identities that this department is assigned to, automatically obtain membership in the object assigned here.
Remove	Use this button to delete selected entitlements . To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 364: Columns

Column	Description
Entitlement	Shows the entitlement's name.
Origin	Shows how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Department (page description)

To open the **Compliance – Department** page go to **Responsibilities** > **My Responsibilities** > **Departments** > select department > **Compliance**.

On the **Compliance – Department** page, you can see the rule violations caused by this department (see Displaying my departments' rule violations on page 229).

The following table gives an overview of the different content on the **Compliance – Department** page.

Table 365: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Department (page description)

To open the **Attestation – Department** page go to **Responsibilities** > **My Responsibilities** > **Departments** > select department > **Attestation**.

On the **Attestation – Department** page, you can:

- Display all attestation cases linked to this department (see Displaying my department attestation cases on page 231)
- Display details of the objects being attested (see Displaying my department attestation cases on page 231)
- Make approval decisions about pending attestation cases (see Approving and denying my department attestation cases on page 234)
- Display attestors of pending attestation cases (see Displaying attestors of my department pending attestation cases on page 233)
- Send reminders to approvers (see Sending reminders about my department pending attestation cases on page 235)

The following tables give you an overview of the various features and content on the **Attestation – Department** page.

Table 366: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my department pending attestation cases on page 233). Then you can send reminder emails to these identities (see Sending reminders about my department pending attestation cases on page 235).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my department pending attestation cases on page 235).
Approve	Opens the **Pending Attestations – Department** page (see Pending attestations – Department (page description) on page 909) Use this button to make approval decisions about attestation cases pending for the department (see Approving and denying my department attestation cases on page 234).

Table 367: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my department pending attestation cases on page 233). Then you can send reminder emails to these identities (see Sending reminders about my department pending attestation cases on page 235).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my department attestation cases on page 231).

Table 368: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane,

Column	Description
	on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Department (page description)

To open the **Risk – Department** page go to **Responsibilities** > **My Responsibilities** > **Departments** > select department > **Risk**.

On the **Risk – Department** page, you can:

- Display the department's calculated risk index (see Displaying my department risk indexes on page 236)
- Show how the calculated risk index is put together (see Displaying my department risk indexes on page 236)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – Department** page.

Table 369: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying my department risk indexes on page 236).

Table 370: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment.

Column	Description
	• At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Department (page description)

Open the **History – Department** page by navigating through **Responsibilities** > **My Responsibilities** > **Departments** > select department > **History**.

On the **History – Department** page, you can show all the department's changes (see My departments' history on page 237).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a department, either on a timeline or in a table (see Displaying my department history on page 238).

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments (see Displaying the status overview of my departments on page 239). It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now (see Comparing statuses of my departments on page 239). You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Department** page.

Table 371: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table	Use this button to display the changes in table form.

Control	Description
view	
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Deselect the check box if you also want to see properties that have not changed since they were created.

Table 372: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now (see Comparing statuses of my departments on page 239). You can also show what the value of the property was at the selected point in time and what the value is now.

Table 373: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.

Column	Description
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Department (page description)

To open the **Usage – Department** page go to **Responsibilities** > **My Responsibilities** > **Departments** > select department > **Usage**.

On the **Usage – Department** page, you can see which roles and organizations that belong to the identities to which this department is assigned (see Displaying role memberships of my department members on page 240).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the various features on the **Usage – System role** page.

Table 374: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to see (see Displaying role memberships of my department members on page 240).
More information	Use this button to show the legend that explains the content of the overview (see Displaying role memberships of my department members on page 240).

Compliance reports – Department (page description)

Open the **Compliance reports – Department** page by navigating through **Responsibilities** > **My Responsibilities** > **Departments** > select department > **Compliance reports**.

On the **Compliance Reports - Department** page you can:

- Display the department's policy violations (see Displaying my department policy violations on page 229)
- Display rule violations of identities that the department is assigned to (see Displaying rule violations of my department members on page 230)
- Display risk indexes and entitlements of identities that the department is assigned to (see Displaying risk indexes and entitlements of my department members on page 230)

The information is divided into three parts:

- **Policy violations**: Shows you all the current policy violations caused by the department.
- **Compliance rule violations**: Shows you the current rule violations of the identities to which the department is assigned.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and authorizations**: Displays all identities to which the department is assigned. Additionally, the number of assigned entitlements and the risk index of these identities are displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – Department** page.

Table 375: Columns

Column	Description
Policy violations	
Violating object	Shows you which object caused the rule violation.
Policy	Shows you the policy that was violated.
Status	Shows you the status of the rule policy.
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows you the violated rule.
Approval state	Shows you how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance –

Column	Description
	Governance Administration on page 209.
Identities: Risk index and entitlements	
Identities	Shows you the identity to which this department is assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Cost centers (page description)

To open the **Cost centers** page go to **Responsibilities** > **My Responsibilities** > **Cost centers**.

On the **Cost centers** page, you can:

- View all the cost centers that you manage (see Displaying my cost centers on page 318)

  Restore deleted cost centers (see Restoring my deleted cost centers on page 319)

If you click a cost center in the list, a new page opens (see Cost center overview page (page description) on page 1091), which contains more information and configuration options for the cost center.

The following tables give you an overview of the different functions and content on the **Cost centers** page.

Table 376: Controls

Control	Description
To restore a deleted role	Use this button to restore a deleted cost center (see Restoring my deleted cost centers on page 319).

Table 377: Columns

Column	Description
Name	Shows the cost center's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Cost center overview page (page description)

To open a cost center's overview page go to **Responsibilities** > **My Responsibilities** > **Cost Centers** and click a cost center.

On the cost center's overview page, you can perform various actions on the cost center you selected beforehand.

To do this, click on one of the tiles:

Table 378: Tiles

Tile	Description
Overview	Opens the **Overview - Cost center** page (see Overview – Cost center (page description) on page 1093). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my cost center overviews on page 320). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Cost center** page (see Main data – Cost center (page description) on page 1093). Here you can see and edit the cost center's main data (see Displaying and editing my cost center main data on page 320).
Memberships	Opens the **Memberships - Cost center** page (see Memberships – Cost center (page description) on page 1094). You select the following actions: • Display identities that are assigned this location (see Displaying memberships in my cost centers on page 321) • Assign identities to the location (see Assigning my identities to cost centers on page 322) • Remove identities from the location (see Removing identities from my cost centers on page 322)
Permissions	Opens the **Entitlements – Cost center** page (see Entitlements – Cost center (page description) on page 1095). You select the following actions: • Display entitlements assigned to the cost center (see Displaying my cost center entitlements on page 323) • Add new entitlements to the cost center (see Adding my cost center entitlements on page 324) • Delete cost center entitlements (see Deleting my cost center entitlements on page 325)
Compliance	Opens the **Compliance – Cost center** page (see Compliance – Cost

Tile	Description
	center (page description) on page 1096). Here you can see rule violations that were caused by this cost center (see Displaying my cost center rule violations on page 332).
Attestation	Opens the **Attestation – Cost center** page (see Attestation – Cost center (page description) on page 1097). You select the following actions: • Display all attestation cases linked to this cost center (see Displaying my cost center attestation cases on page 326) • Display details of the objects being attested (see Displaying my cost center attestation cases on page 326) • Make approval decisions about pending attestation cases (see Approving and denying my cost center attestation cases on page 328) • Display attestors of pending attestation cases (see Displaying attestors of my cost center pending attestation cases on page 327) • Send reminders to approvers (see Sending reminders about my cost centers' pending attestation cases on page 329)
Risk	Opens the **Risk – Cost center** page (see Risk – Cost center (page description) on page 1099). Here you can see the cost center's risk index (see Displaying my cost center risk indexes on page 334). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – Cost center** page (see History – Cost center (page description) on page 1100). Here you can see all the changes made to the cost center (see My cost center history on page 335).
Usage	Opens the **Usage – Cost center** page (see Usage – Cost center (page description) on page 1102). Here you can see which roles and organizations belong to members of the cost center (see Displaying role memberships of my cost center members on page 338).
Compliance reports	Opens the **Compliance report – Cost center** page (see Compliance reports – Cost center (page description) on page 1102). You select the following actions: • Display the cost center's policy violations (see Displaying my cost center policy violations on page 332)

Tile	Description
	• Display rule violations of identities that the cost center is assigned to (see Displaying rule violations of my cost center members on page 333) • Display risk indexes and entitlements of identities that the cost center is assigned to (see Displaying risk indexes and entitlements of my cost center members on page 333)
Split	You can copy or move memberships and entitlements from the cost center to a new role (department, business role, cost center, location) (see Copying/splitting my cost centers on page 339).
Compare and merge	You can copy or move properties of the cost center to another role (department, business role, cost center, location) for which you are responsible, compare them and then select the properties you require and merge them (see Comparing and merging my cost centers on page 340).
Redo	Here you can restore a deleted cost center that was under this cost center (see Restoring my deleted cost centers on page 319).
Statistics	Here you can see various statistics about the cost center (see Displaying my cost center statistics on page 341).

Overview – Cost center (page description)

To open the **Overview – Cost center** page go to **Responsibilities** > **My Responsibilities** > **Cost centers** > select cost center > **Overview**.

On the **Overview – Cost center** page, you can see all the information relevant to the cost center summarized in an overview (see Displaying my cost center overviews on page 320.)

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Cost center (page description)

To open the **Main data – Cost center** page go to **Responsibilities** > **My Responsibilities** > **Cost centers** > select cost center > **Main data**.

On the **Main data - Cost center** page, you can show and edit the cost center's main data (see Displaying and editing my cost center main data on page 320).

The following tables give you an overview of the different functions and content on the **Main data – Cost center** page.

Table 379: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 380: Cost center main data

Property	Description
Cost center	Enter a full, descriptive name for the cost center.
Short name	Enter a short name for the cost center.
Parent cost center	Click **Assign**/**Change** and select a cost center to be the parent cost center for organizing the cost center hierarchically. If you want the cost center at the root of a cost center hierarchy, leave the field empty.
Manager	Click **Assign**/**Change** and select the manager responsible for the cost center.
2nd Manager	Click **Assign**/**Change** and select an identity to act as a deputy to the cost center's manager.
Attestors	Click **Assign**/**Change** and select a cost center. Members of the selected application role can approve attestation cases for the cost center.
Department	Click **Assign**/**Change** and select the department that the cost center is primarily assigned to.
Location	Click **Assign**/**Change** and select the location the cost center is primarily assigned to.
Role approver	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the cost center.
Role approver (IT)	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the cost center.
Description	Enter a description for the cost center.

Memberships – Cost center (page description)

To open the **Memberships – Cost center** page go to **Responsibilities** > **My Responsibilities** > **Cost centers** > select cost center > **Memberships**.

On the **Memberships - Cost center** page, you can:

- Display identities that are assigned this location (see Displaying memberships in my cost centers on page 321)
- Assign identities to the location (see Assigning my identities to cost centers on page 322)
- Remove identities from the location (see Removing identities from my cost centers on page 322)

The following tables give you an overview of the different functions and content on the **Memberships – Cost center** page.

Table 381: Controls

Control	Description
Request memberships	Use this button to request membership in the cost center for identities (see Assigning my identities to cost centers on page 322).
Deleting memberships	Use this button to delete membership in the cost center for selected identities (see Removing identities from my cost centers on page 322). Select the check box in front of the identities whose membership in the cost center you want to delete and click this button.

Table 382: Columns

Column	Description
Identity	Shows you the name of the identity assigned to the cost center.
Origin	Shows you whether the cost center of the identity was assigned directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Cost center (page description)

To open the **Entitlements – Cost center** page go to **Responsibilities** > **My Responsibilities** > **Cost centers** > select cost center > **Entitlements**.

On the **Entitlements – Cost center** page, you can:

- Display entitlements assigned to the cost center (see Displaying my cost center entitlements on page 323)
- Add new entitlements to the cost center (see Adding my cost center entitlements on page 324)

- Delete cost center entitlements (see Deleting my cost center entitlements on page 325)

The following tables give you an overview of the different functions and content on the **Entitlements – Cost center** page.

Table 383: Controls

Control	Description
New	Use this button to add a new entitlement to the cost center (see Adding my cost center entitlements on page 324). Identities that this cost center is assigned to, automatically obtain membership in the object assigned here.
Remove	Use this button to delete selected entitlements . To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 384: Columns

Column	Description
Entitlement	Shows the entitlement's name.
Origin	Shows how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Cost center (page description)

To open the **Compliance – Cost center** page go to **Responsibilities** > **My Responsibilities** > **Cost centers** > select cost center > **Compliance**.

On the **Compliance – Cost center** page, you can see the rule violations caused by this cost center (see Displaying my cost center rule violations on page 332).

The following table gives an overview of the different content on the **Compliance – Cost center** page.

Table 385: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.

Column	Description
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Cost center (page description)

To open the **Attestation – Cost center** page go to **Responsibilities** > **My Responsibilities** > **Cost centers** > select cost center > **Attestation**.

On the **Attestation – Cost center** page, you can:

- Display all attestation cases linked to this cost center (see Displaying my cost center attestation cases on page 326)
- Display details of the objects being attested (see Displaying my cost center attestation cases on page 326)
- Make approval decisions about pending attestation cases (see Approving and denying my cost center attestation cases on page 328)
- Display attestors of pending attestation cases (see Displaying attestors of my cost center pending attestation cases on page 327)
- Send reminders to approvers (see Sending reminders about my cost centers' pending attestation cases on page 329)

The following tables give you an overview of the various features and content on the **Attestation – Cost center** page.

Table 386: Controls

Control	Description
View approvers for pending	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my cost

Control	Description
cases	center pending attestation cases on page 327). Then you can send reminder emails to these identities (see Sending reminders about my cost centers' pending attestation cases on page 329).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my cost centers' pending attestation cases on page 329).
Approve	Opens the **Pending Attestations – Cost center** page (see Pending attestations – Cost center (page description) on page 935). Use this button to make approval decisions about attestation cases pending for the cost center (see Approving and denying my cost center attestation cases on page 328).

Table 387: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my cost center pending attestation cases on page 327). Then you can send reminder emails to these identities (see Sending reminders about my cost centers' pending attestation cases on page 329).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my cost center attestation cases on page 326).

Table 388: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on

Column	Description
	the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Cost center (page description)

To open the **Risk – Cost center** page go to **Responsibilities** > **My Responsibilities** > **Cost centers** > select cost center > **Risk**.

On the **Risk – Cost center** page, you can:

- Display the cost center's calculated risk index (see Displaying my cost center risk indexes on page 334)
- Show how the calculated risk index is put together (see Displaying my cost center risk indexes on page 334)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – Cost center** page.

Table 389: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying my cost center risk indexes on page 334).

Table 390: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.

Column	Description
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Cost center (page description)

Open the **History – Cost center** page by navigating through **Responsibilities** > **My Responsibilities** > **Cost centers** > select cost center > **History**.

On the **History – Cost center** page, you can show all the cost center's changes (see My cost center history on page 335).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a cost center, either on a timeline or in a table (see Displaying my cost center history on page 335).

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments (see Displaying the status overview of my cost centers on page 336). It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now (see Comparing statuses of my cost centers on page 337). You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Cost center** page.

Table 391: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to	Use this button to display the changes as a timeline.

Control	Description
timeline view	
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Deselect the check box if you also want to see properties that have not changed since they were created.

Table 392: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now (see Comparing statuses of my cost centers on page 337). You can also show what the value of the property was at the selected point in time and what the value is now.

Table 393: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	

Column	Description
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Cost center (page description)

To open the **Usage – Cost center** page go to **Responsibilities** > **My Responsibilities** > **Cost centers** > select cost center > **Usage**.

On the **Usage – Cost center** page, you can see the roles and organizations that belong to the identities to which this cost center is assigned (see Displaying role memberships of my cost center members on page 338).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the various features on the **Usage – Cost center** page.

Table 394: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to see (see Displaying role memberships of my cost center members on page 338).
More information	Use this button to show the legend that explains the content of the overview (see Displaying role memberships of my cost center members on page 338).

Compliance reports – Cost center (page description)

Text

Locations (page description)

To open the **Locations** page go to **Responsibilities** > **My Responsibilities** > **Locations**.

On the **Locations** page, you can:

- View all the locations that you manage (see Displaying my locations on page 384)
- Restore deleted locations (see Restoring my deleted locations on page 384)

If you click a location in the list, a new page opens (see Location overview page (page description) on page 1103), which contains more information and configuration options for the location.

The following tables give you an overview of the different functions and content on the **Locations** page.

Table 395: Controls

Control	Description
To restore a deleted role	Use this button to restore a deleted location (see Restoring my deleted locations on page 384).

Table 396: Columns

Column	Description
Name	Shows the location's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Location overview page (page description)

To open a location's overview page go to **Responsibilities** > **My Responsibilities** > **Locations** and click a location.

On the location's overview page, you can perform various actions on the location you selected.

To do this, click on one of the tiles:

Table 397: Tiles

Tile	Description
Overview	Opens the **Overview - Location** page (see Overview - Location (page description) on page 1106). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my locations' overviews on page 385). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Location** page (see Main data - Location (page description) on page 1106). Here you can see and edit the location's main data (see Displaying and

Tile	Description
	editing my locations' main data on page 386).
Memberships	Opens the **Memberships – Location** page (see Memberships – Location (page description) on page 1107). You select the following actions: • Display identities assigned to the location (see Displaying memberships in my locations on page 387) • Assign identities to the location (see Assigning identities to my locations on page 387) • Remove identities from the location (see Removing identities from my locations on page 388)
Permissions	Opens the **Entitlements – Location** (see Entitlements – Location (page description) on page 1108). You select the following actions: • Display entitlements assigned to the location (see Displaying my locations' entitlements on page 389) • Add new entitlements to the location (see Adding my locations' entitlements on page 390) • Delete the location's entitlements/memberships (see Deleting my locations' entitlements on page 390)
Compliance	Opens the **Compliance – Location** page (see Compliance – Location (page description) on page 1109). Here you can see rule violations that were caused by this location (see Displaying my locations' rule violations on page 397).
Attestation	Opens the **Attestations – Location** (see Attestation – Location (page description) on page 1110). You select the following actions: • Display all attestation cases linked to this location (see Displaying my locations' attestation cases on page 391) • Display details of the objects being attested (see Displaying my locations' attestation cases on page 391) • Make approval decisions about pending attestation cases (see Approving and denying my locations' attestation cases on page 394) • Display attestors of pending attestation cases (see Displaying attestors of my locations' pending attestation cases on page 393) • Send reminders to approvers (see Sending reminders about my locations' pending attestation cases on page 395)

Tile	Description
Risk	Opens the **Risk – Location** page (see Risk – Location (page description) on page 1111). Here you can see the location's risk index (see Displaying my locations' risk indexes on page 399). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – Location** page (see History – Location (page description) on page 1112). Here you can see all the changes made to the location (see My locations' history on page 400).
Usage	Opens the **Usage – Location** page (see Usage – Location (page description) on page 1114). Here you can see which roles and organizations belong to members of the location (see Displaying role memberships of my locations' members on page 403).
Compliance reports	Opens the **Compliance report – Location** page (see Compliance reports - Location (page description) on page 1115). You select the following actions: • Display the location's policy violations (see Displaying my locations' policy violations on page 398) • Display rule violations of identities that the locatiois assigned to (see Displaying rule violations of my locations' members on page 398) • Display risk indexes and entitlements of identities that the location is assigned to (see Displaying risk indexes and entitlements of my locations' members on page 399)
Split	You can copy or move memberships and entitlements from the location to a new role (department, business role, cost center, location) (see Copying/splitting my locations on page 404).
Compare and merge	You can copy or move properties of the location to another role (department, business role, cost center, location) for which you are responsible, compare them and then select the properties you require and merge them (see Comparing and merging my locations on page 405).
Redo	Here you can restore a deleted location that was under this location (see Restoring my deleted locations on page 384).
Statistics	Here you can see various statistics about the location (see Displaying my cost center statistics on page 341).

Overview - Location (page description)

To open the **Overview – Location** page go to **Responsibilities** > **My Responsibilities** > **Locations** > select location > **Overview**.

On the **Overview - Location** page, you can see all the information relevant to the location summarized in an overview (see Displaying my locations' overviews on page 385).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data - Location (page description)

To open the **Main data – Location** page go to **Responsibilities** > **My Responsibilities** > **Locations** > select location > **Main data**.

On the **Main data - Location** page, you can show and edit the location's main data (see Displaying and editing my locations' main data on page 386).

The following tables give you an overview of the different functions and content on the **Main data – Location** page.

Table 398: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 399: Location main data

Property	Description
Location	Enter a full, descriptive name for the location.
Short name	Enter a short name for the location.
Name	Enter an additional description for the location.
Parent location	Click **Assign**/**Change** and select a location to be the parent location for organizing the location hierarchically. If you want the location at the root of a location hierarchy, leave the field empty.
Manager	Click **Assign**/**Change** and select the manager responsible for the location.
2nd Manager	Click **Assign**/**Change** and select an identity to act as a deputy to the location's manager.
Attestors	Click **Assign**/**Change** and select a cost center. Members of the selected application role can approve attestation cases for the location.
Department	Click **Assign**/**Change** and select the department the location is primarily assigned to.

Property	Description
Cost center	Click **Assign**/**Change** and select the cost center the location is primarily assigned to.
Role approver	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the location.
Role approver (IT)	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the location.
Description	Enter a description for the location.

Memberships – Location (page description)

To open the **Memberships – Location** page go to **Responsibilities** > **My Responsibilities** > **Locations** > select location > **Memberships**.

On the **Memberships - Location** page, you can:

- Display identities assigned to the location (see Displaying memberships in my locations on page 387)
- Assign identities to the location (see Assigning identities to my locations on page 387)
- Remove identities from the location (see Removing identities from my locations on page 388)

The following tables give you an overview of the different functions and content on the **Memberships – Location** page.

Table 400: Controls

Control	Description
Request memberships	Use this button to request in the location assignment for identities (see Assigning identities to my locations on page 387).
Deleting memberships	You can use this button to delete the assignment to the location for selected identities (see Removing identities from my locations on page 388). Select the check boxes in front of the identities whose locations you want to delete and click this button.

Table 401: Columns

Column	Description
Identity	Shows you the name of the identity assigned to the location.
Origin	Shows you whether the location of the identity was assigned directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Location (page description)

To open the **Entitlements – Location** page go to **Responsibilities** > **My Responsibilities** > **Locations** > select location > **Entitlements**.

On the **Entitlements – Location** page, you can:

- Display entitlements assigned to the location (see Displaying my locations' entitlements on page 389)
- Add new entitlements to the location (see Adding my locations' entitlements on page 390)
- Delete the location's entitlements/memberships (see Deleting my locations' entitlements on page 390)

The following tables give you an overview of the different functions and content on the **Entitlements – Location** page.

Table 402: Controls

Control	Description
New	Use this button to add a new entitlement to the location (see Adding my locations' entitlements on page 390). Identities that this location is assigned to, automatically obtain membership in the object assigned here.
Remove	Use this button to delete selected entitlements . To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 403: Columns

Column	Description
Entitlement	Shows the entitlement's name.
Origin	Shows how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Location (page description)

To open the **Compliance – Location** page go to **Responsibilities** > **My Responsibilities** > **Locations** > select location > **Compliance**.

On the **Compliance – Location** page, you can see the rule violations caused by the location (see Displaying my locations' rule violations on page 397).

The following table gives an overview of the different content on the **Compliance – Location** page.

Table 404: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Location (page description)

To open the **Attestation – Location** page go to **Responsibilities** > **My Responsibilities** > **Locations** > select location > **Attestation**.

On the **Attestation – Location** page, you can:

- Display all attestation cases linked to this location (see Displaying my locations' attestation cases on page 391)
- Display details of the objects being attested (see Displaying my locations' attestation cases on page 391)
- Make approval decisions about pending attestation cases (see Approving and denying my locations' attestation cases on page 394)
- Display attestors of pending attestation cases (see Displaying attestors of my locations' pending attestation cases on page 393)
- Send reminders to approvers (see Sending reminders about my locations' pending attestation cases on page 395)

The following tables give you an overview of the various features and content on the **Attestation – Location** page.

Table 405: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my locations' pending attestation cases on page 393). Then you can send reminder emails to these identities (see Sending reminders about my locations' pending attestation cases on page 395).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my locations' pending attestation cases on page 395).
Approve	Opens the **Pending Attestations – Locations** page (see Pending attestations – Location (page description) on page 916). Use this button to make approval decisions about attestation cases pending for the location (see Approving and denying my locations' attestation cases on page 394).

Table 406: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my locations' pending attestation cases on page 393). Then you can send reminder emails to these identities (see Sending reminders about my

Control	Description
	locations' pending attestation cases on page 395).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my locations' attestation cases on page 391).

Table 407: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Location (page description)

To open the **Risk – Location** page go to **Responsibilities** > **My Responsibilities** > **Locations** > select location > **Risk**.

On the **Risk – Location** page, you can:

- Display the location's calculated risk index (see Displaying my locations' risk indexes on page 399)
- Show how the calculated risk index is put together (see Displaying my locations' risk indexes on page 399)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – Location** page.

Table 408: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying my locations' risk indexes on page 399).

Table 409: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Location (page description)

Open the **History – Location** page by navigating through **Responsibilities** > **My Responsibilities** > **Locations** > select location > **History**.

On the **History – Location** page, you can show all the location's changes (see My locations' history on page 400).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a location, either on a timeline or in a table (see Displaying my locations' history on page 401).

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments (see Displaying the status overview of my locations on page 402). It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

- **Status comparison**: You can select a date and display all the changes made from then until now (see Comparing statuses of my locations on page 402). You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Location** page.

Table 410: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Deselect the check box if you also want to see properties that have not changed since they were created.

Table 411: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now (see Comparing statuses of my locations on page 402). You can also show what the value of the property was at the selected point in time and what the value is now.

Table 412: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.

Column	Description
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Location (page description)

To open the **Usage – Location** page go to **Responsibilities** > **My Responsibilities** > **Locations** > select location > **Usage**.

On the **Usage – Location** page, you can see which roles and organizations that belong to the identities to which this location is assigned (see Displaying role memberships of my locations' members on page 403).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the various features on the **Usage – Location** page.

Table 413: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to see (see Displaying role memberships of my locations' members on page 403).
More information	Use this button to show the legend that explains the content of the overview (see Displaying role memberships of my locations' members on page 403).

Compliance reports - Location (page description)

Open the **Compliance reports – Location** page by navigating through **Responsibilities** > **My Responsibilities** > **Locations** > select location > **Compliance reports**.

On the **Compliance Reports - Location** page you can:

- Display the location's policy violations (see Displaying my locations' policy violations on page 398)
- Display rule violations of identities that the locatiois assigned to (see Displaying rule violations of my locations' members on page 398)
- Display risk indexes and entitlements of identities that the location is assigned to (see Displaying risk indexes and entitlements of my locations' members on page 399)

The information is divided into three parts:

- **Policy violations**: Shows you all the current policy violations caused by the location.
- **Compliance rule violations**: Shows you the current rule violations of the identities to which the location is assigned.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and authorizations**: Displays all identities to which the location is assigned. Additionally, the number of assigned entitlements and the risk index of these identities are displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – Location** page.

Table 414: Columns

Column	Description
Policy violations	
Violating object	Shows you which object caused the rule violation.
Policy	Shows you the policy that was violated.
Status	Shows you the status of the rule policy.

Column	Description
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows you the violated rule.
Approval state	Shows you how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.
Identities: Risk index and entitlements	
Identities	Shows you the identity to which this location is assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Application roles (page description)

To open the **One Identity Manager application roles** page go to **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles**.

Use application roles to quickly and simply assign entitlement profiles to identities that match their tasks and functions. One Identity Manager already supplies a number of default application roles. You can also create custom application roles to suit your own needs.

On the **One Identity Manager applications roles** page, you can:

- View all the application roles that you manage (see Displaying my application roles on page 245)
- Create new application roles (see Creating your own application roles on page 246)

If you click an application role in the list, a new page opens (see Application role overview page (page description) on page 1118), which contains more information and configuration options for the application role.

The following tables give you an overview of the different functions and content on the **One Identity Manager application roles** page.

Table 415: Controls

Control	Description
New application role	Opens the **Create a new application role** page (see Creating new application roles (see (page description)) on page 1117). Use this button to add a new application role to the system (see Creating your own application roles on page 246).

Table 416: Columns

Column	Description
Name	Shows the application role's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Creating new application roles (see (page description))

To open the **Create a new application role** page go to **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles** > **New application role**.

On the **Create new application role** page, you can create a new application role for which you are responsible. Do this by entering the new application role's main data (see Creating your own application roles on page 246).

Enter the following main data.

Table 417: Main data of application roles

Property	Description
Application role	Enter a full, descriptive name for the application role.
Internal name	Enter a company internal name for the application role.
Parent application role	Click **Assign/Change** and select an application role to be the parent application role to organize the application role hierarchically. If you want the application role at the root of an application role hierarchy, leave the field empty.
Manager	Click **Assign/Change** and select the manager responsible for the application role.
2nd Manager	Click **Assign/Change** and select an identity to act as a deputy to the application role's manager.

Property	Description
Description	Enter a description for the application role.
Comment	Enter a comment for the application role.
Full name	Shows the full name of the application role, which is automatically made up of the identifiers of the application role and the parent application role.
Department	Click **Assign/Change** and select a department for the application role.
Location	Click **Assign/Change** and select a location for the application role.
Cost center	Click **Assign/Change** and select a cost center for the application role.

Application role overview page (page description)

To open an application role's overview page go to **Responsibilities** > **My Responsibilities** > **One Identity Manager Application Roles** and click an application role.

On the application role's overview page, you can perform various actions on the application you selected beforehand.

To do this, click on one of the tiles:

Table 418: Tiles

Tile	Description
Overview	Opens the **Overview - Application role** page (see Overview – Application role (page description) on page 1120). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my application roles' overviews on page 245). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Application role** page (see Main data - Application role (page description) on page 1120). Here you can see and edit the application role's main data (see Displaying and editing my application roles' main data on page 246).
Memberships	Opens the **Memberships – Application role** page (see Memberships – Application role (page description) on page 1121). You select the following actions: • Display employees that are assigned this application role (see Displaying memberships in my application roles on page 247) • Request the application role for identities (see Assigning identities to my application roles on page 247) • Cancel the application role for identities (see Removing identities

Tile	Description
	from my application roles on page 248)
Permissions	Opens the **Entitlements – Application role** (see Entitlements – Application role (page description) on page 1122). You select the following actions: • Display reports assigned to this application role (see Displaying my application roles' reports on page 249)
Attestation	Opens the **Attestations – Application role** (see Attestation – Application role (page description) on page 1123). You select the following actions: • Display all attestation cases linked to this application role (see Displaying my application roles' pending attestation cases on page 253) • Display details of the objects being attested (see Displaying my application roles' pending attestation cases on page 253) • Make approval decisions about pending attestation cases (see Approving and denying my application roles' attestation cases on page 255) • Display attestors of pending attestation cases (see Displaying attestors of my application roles' pending attestation cases on page 254) • Send reminders to approvers (see Sending reminders about my application roles' pending attestation cases on page 256)
History	Opens the **History – Application role** page (see History – Application role (page description) on page 1125). Here you can see all the changes made to the application role (see My application roles' history on page 258).
Usage	Opens the **Usage – Application role** page (see Usage – Application role (page description) on page 1127). Here you can see which roles and organizations belong to members of the application role (see Displaying role memberships of my application roles' members on page 261).
Compliance reports	Opens the **Compliance report – Application role** page (see Compliance reports – Application role (page description) on page 1127). You select the following actions: • Display the application role's policy violations (see Displaying my application roles' policy violations on page 250) • Display rule violations of identities that the application role is

Tile	Description
	assigned to (see Displaying rule violations of my application roles' members on page 251) • Display risk indexes and entitlements of identities that the application role is assigned to (see Displaying risk indexes and entitlements of my application roles' members on page 251)

Overview – Application role (page description)

To open the **Overview – Application role** page go to **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles** > select application role > **Overview**.

On the **Overview – Application role** page, you can see all the information relevant to the application role summarized in an overview (see Displaying my application roles' overviews on page 245).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data - Application role (page description)

Open the **Main data – Application role** page by navigating through **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles** > select application role > **Main data**.

On the **Main data - application role** page, you can show and edit the application role's main data (see Displaying and editing my application roles' main data on page 246).

The following tables give you an overview of the different functions and content on the **Main data – One Identity Manager application role** page.

Table 419: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 420: Main data of application roles

Property	Description
Application role	Enter a full, descriptive name for the application role.
Internal name	Enter a company internal name for the application role.
Parent	Click **Assign/Change** and select an application role to be the parent

Property	Description
application role	application role to organize the application role hierarchically. If you want the application role at the root of an application role hierarchy, leave the field empty.
Manager	Click **Assign**/**Change** and select the manager responsible for the application role.
2nd Manager	Click **Assign**/**Change** and select an identity to act as a deputy to the application role's manager.
Description	Enter a description for the application role.
Comment	Enter a comment for the application role.
Full name	Shows the full name of the application role, which is automatically made up of the identifiers of the application role and the parent application role.
Department	Click **Assign**/**Change** and select a department for the application role.
Location	Click **Assign**/**Change** and select a location for the application role.
Cost center	Click **Assign**/**Change** and select a cost center for the application role.

Memberships – Application role (page description)

To open the **Memberships – Application role** page go to **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles** > select application role > **Memberships**.

On the **Memberships - Application role** page, you can:

- Display employees that are assigned this application role (see Displaying memberships in my application roles on page 247)
- Request the application role for identities (see Assigning identities to my application roles on page 247)
- Cancel the application role for identities (see Removing identities from my application roles on page 248)

The following tables give you an overview of the different functions and content on the **Memberships – Application role** page.

Table 421: Controls

Control	Description
Request memberships	Use this button to request the application role for identities (see Assigning identities to my application roles on page 247).
Deleting memberships	Use this button to delete the application role's assignment for selected identities (see Removing identities from my application roles on page 248).

Control	Description
	Select the check box in front of the identities whose membership in the application role you want to delete and click this button.

Table 422: Columns

Column	Description
Identity	Shows you the name of the identity to which the application role is assigned.
Origin	Shows you whether the application role was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Application role (page description)

To open the **Entitlements – Application role** page go to **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles** > select application role > **Entitlements**.

On the **Entitlements – Application role** page, you can:

- Display reports assigned to this application role (see Displaying my application roles' reports on page 249)

The following tables give you an overview of the different functions and content on the **Entitlements – One Identity Manager application roles** page.

Table 423: Columns

Column	Description
Entitlement	Shows you the report's name.

Column	Description
Origin	Shows you how the entitlement was assigned.
Entitlement type	Shows the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Application role (page description)

To open the **Attestation – Application role** page go to **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles** > select application role > **Attestation**.

On the **Attestation – Application role** page, you can:

- Display all attestation cases linked to this application role (see Displaying my application roles' pending attestation cases on page 253)
- Display details of the objects being attested (see Displaying my application roles' pending attestation cases on page 253)
- Make approval decisions about pending attestation cases (see Approving and denying my application roles' attestation cases on page 255)
- Display attestors of pending attestation cases (see Displaying attestors of my application roles' pending attestation cases on page 254)
- Send reminders to approvers (see Sending reminders about my application roles' pending attestation cases on page 256)

The following tables give you an overview of the various features and content on the **Attestation – <One Identity Manager application role** page.

Table 424: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my application roles' pending attestation cases on page 254). Then you can send reminder emails to these identities (see Sending reminders about my application roles' pending attestation cases on page 256).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my application roles' pending attestation cases on page 256).
Approve	Opens the **Pending Attestations – One Identity Manager Application roles** page (see Pending attestations – Application role (page description) on page 905).

Control	Description
	Use this button to make approval decisions about attestation cases pending for the application role (see Approving and denying my application roles' attestation cases on page 255).

Table 425: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my application roles' pending attestation cases on page 254). Then you can send reminder emails to these identities (see Sending reminders about my application roles' pending attestation cases on page 256).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my application roles' pending attestation cases on page 253).

Table 426: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

History – Application role (page description)

Open the **History – Application role** page by navigating through **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles** > select application role > **History**.

On the **History – Application role** page, you can show all the application role's changes (see My application roles' history on page 258).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect an application role, either on a timeline or in a table (see Displaying my application roles' history on page 258).

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.
- **Status overview**: Shows an overview of all assignments (see Displaying the status overview of my application roles on page 259). It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now (see Comparing statuses of my application roles on page 260). You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Application role** page.

Table 427: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.

Control	Description
Display changed values only	Deselect the check box if you also want to see properties that have not changed since they were created.

Table 428: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now (see Comparing statuses of my application roles on page 260). You can also show what the value of the property was at the selected point in time and what the value is now.

Table 429: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.

Column	Description
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Application role (page description)

Open the **Usage – Application role** page by navigating through **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles** > select application role > **Usage**.

On the **Usage – Application role** page, you can see the roles and organizations that belong to the identities to which this application role is assigned (see Displaying role memberships of my application roles' members on page 261).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the various features on the **Usage – Application role** page.

Table 430: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to see (see Displaying role memberships of my application roles' members on page 261).
More information	Use this button to show the legend that explains the content of the overview (see Displaying role memberships of my application roles' members on page 261).

Compliance reports – Application role (page description)

To open the **Compliance Reports – Application role** page go to **Responsibilities** > **My Responsibilities** > **One Identity Manager application roles** > select application role > **Compliance Reports**.

On the **Compliance Reports - Application role** page you can:

- Display the application role's policy violations (see Displaying my application roles' policy violations on page 250)
- Display rule violations of identities that the application role is assigned to (see Displaying rule violations of my application roles' members on page 251)

- Display risk indexes and entitlements of identities that the application role is assigned to (see Displaying risk indexes and entitlements of my application roles' members on page 251)

The information is divided into three parts:

- **Policy violations**: Shows you all the current policy violations caused by the application role.
- **Compliance rule violations**: Shows you the current rule violations of the identities to which the application role is assigned.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and authorizations**: Displays all identities to which the application role is assigned. Additionally, the number of assigned entitlements and the risk index of these identities are displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – Application role** page.

Table 431: Columns

Column	Description
Policy violations	
Violating object	Shows you which object caused the rule violation.
Policy	Shows you the policy that was violated.
Status	Shows you the status of the rule policy.
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows you the violated rule.
Approval state	Shows you how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.
Identities: Risk index and entitlements	
Identities	Shows you the identity to which this application is assigned.

Column	Description
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Resources (page description)

To open the **Resources** page go to **Responsibilities** > **My Responsibilities** > **Resources**.

On the **Resources** page, you can:

- View all the resources roles that you manage (see Displaying my resources on page 362)
- Create new resource (see Creating your own resources on page 363)

If you click a resource in the list, a new page opens (see Resource overview page (page description) on page 1130), which contains more information and configuration options for the resource.

The following tables give you an overview of the different functions and content on the **Resources** page.

Table 432: Controls

Control	Description
New resources	Opens the **Create a new resource** page (see New resources (page description) on page 1129). Use this button to add a new resource to the system (see Creating your own resources on page 363).

Table 433: Columns

Column	Description
Name	Shows the resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

New resources (page description)

To open the **Create a new resource** page go to **Responsibilities** > **My Responsibilities** > **Resources** > **New resource**.

On the **Create a new resource** page you can create a new resource for which you are responsible. Do this by entering the new resource's main data (see Creating your own resources on page 363).

Enter the following main data.

Table 434: Resource main data

Property	Description
Resource	Enter a full, descriptive name for the resource.
Resource type	Select a resource type for the resource. Use resource types to group resources.
Description	Enter a description for the resource.
IT shop	Select the check box if the resource can also be requested through the IT Shop. The resource can be requested by identities through the Web Portal and the request granted by a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the resource can only be requested through the IT Shop. The resource can be requested by identities through the Web Portal and the request granted by a defined approval process. It is not possible to assign the resource directly to roles outside the IT Shop (for example, in Manager).
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use an assignment resource until a service item has been assigned to it.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning resources to identities. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Resource overview page (page description)

To open a resource's overview page go to **Responsibilities** > **My Responsibilities** > **Resources** and click a resource.

On the resource's overview page, you can perform various actions on the resource you selected beforehand.

To do this, click on one of the tiles:

Table 435: Tiles

Tile	Description
Overview	Opens the **Overview - Resource** page (see Overview – Resource (page description) on page 1132). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my resources' overviews on page 362). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Resource** page (see Main data – Resource (page description) on page 1132). Here you can see and edit the resource's main data (see Displaying and editing my resources' main data on page 363).
Memberships	Opens the **Memberships – Resource** page (see Memberships – Resource (page description) on page 1133). You select the following actions: • Display identities that are assigned this resource (see Displaying memberships in my resources on page 364) • Request the resource for identities (see Assigning identities to my resources on page 364) • Cancel this resource for identities (see Removing identities from my resources on page 365)
Attestation	Opens the **Attestations – Resource** (see Attestation - Resource (page description) on page 1134). You select the following actions: • Display all attestation cases linked to this resource (see Displaying my resources' attestation cases on page 366) • Display details of the objects being attested (see Displaying my resources' attestation cases on page 366) • Make approval decisions about pending attestation cases (see Approving and denying my resources' attestation cases on page 368) • Display attestors of pending attestation cases (see Displaying attestors of my resources' pending attestation cases on page 367) • Send reminders to approvers (see Sending reminders about my resources' pending attestation cases on page 370)
Usage	Opens the **Usage – Resource** page (see Usage – Resource (page description) on page 1136). Here you can see which roles and organizations belong to members of the resource (see Displaying role memberships of my resources' members on page 371).

Overview – Resource (page description)

To open the **Overview – Resource** page go to **Responsibilities** > **My Responsibilities** > **Resources** > select resource > **Overview**.

On the **Overview – Resource** page, you can see all the information relevant to the resource summarized in an overview (see Displaying my resources' overviews on page 362).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Resource (page description)

To open the **Main data – Resource** page go to **Responsibilities** > **My Responsibilities** > **Resources** > select resource > **Main data**.

On the **Main data - Resource** page, you can show and edit the resource's main data (see Displaying and editing my resources' main data on page 363).

The following tables give you an overview of the different functions and content on the **Main data – Resource** page.

Table 436: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 437: Resource main data

Property	Description
Resource	Enter a full, descriptive name for the resource.
Resource type	Select a resource type for the resource. Use resource types to group resources.
Description	Enter a description for the resource.
IT shop	Select the check box if the resource can also be requested through the IT Shop. The resource can be requested by identities through the Web Portal and the request granted by a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the resource can only be requested through the IT Shop. The resource can be requested by identities through the Web Portal and the request granted by a defined approval process. It is not possible to assign the resource directly to roles outside the IT Shop (for example, in Manager).

Property	Description
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use an assignment resource until a service item has been assigned to it.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning resources to identities. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Memberships – Resource (page description)

To open the **Memberships – Resource** page go to **Responsibilities** > **My Responsibilities** > **Resources** > select resource > **Memberships**.

On the **Memberships - Resource** page, you can:

- Display identities that are assigned this resource (see Displaying memberships in my resources on page 364)
- Request the resource for identities (see Assigning identities to my resources on page 364)
- Cancel this resource for identities (see Removing identities from my resources on page 365)

The following tables give you an overview of the different functions and content on the **Memberships – Resource** page.

Table 438: Controls

Control	Description
Request memberships	Use this button to request the resource for identities (see Assigning identities to my resources on page 364).
Deleting memberships	You can use this button to delete the resource assignment for selected identities (see Removing identities from my resources on page 365). Select the check boxes in front of the identities whose resource assignments you want to delete and click this button.

Table 439: Columns

Column	Description
Identity	Shows you the name of the identity to which the resource is assigned.
Origin	Shows you whether the resource was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation - Resource (page description)

To open the **Attestation – Resource** page go to **Responsibilities** > **My Responsibilities** > **Resources** > select resource > **Attestation**.

On the **Attestation – Resource** page, you can:

- Display all attestation cases linked to this resource (see Displaying my resources' attestation cases on page 366)
- Display details of the objects being attested (see Displaying my resources' attestation cases on page 366)
- Make approval decisions about pending attestation cases (see Approving and denying my resources' attestation cases on page 368)
- Display attestors of pending attestation cases (see Displaying attestors of my resources' pending attestation cases on page 367)
- Send reminders to approvers (see Sending reminders about my resources' pending attestation cases on page 370)

The following tables give you an overview of the various features and content on the **Attestation – Resource** page.

Table 440: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my resources' pending attestation cases on page 367). Then you can send reminder emails to these identities (see Sending reminders about my resources' pending attestation cases on page 370).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending

Control	Description
	reminders about my resources' pending attestation cases on page 370).
Approve	Opens the **Pending Attestations – Resources** page (see Pending attestations – Resource (page description) on page 947). Use this button to make approval decisions about attestation cases pending for the resource (see Approving and denying my resources' attestation cases on page 368).

Table 441: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my resources' pending attestation cases on page 367). Then you can send reminder emails to these identities (see Sending reminders about my resources' pending attestation cases on page 370).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my resources' attestation cases on page 366).

Table 442: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.

Column	Description
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Resource (page description)

To open the **Usage – Resource** page go to **Responsibilities** > **My Responsibilities** > **Resources** > select resource > **Usage**.

On the **Usage – Resource** page, you can see the roles and organizations that belong to the identities to which this resource is assigned (see Displaying role memberships of my resources' members on page 371).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the various features on the **Usage – Resources** page.

Table 443: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to see (see Displaying role memberships of my resources' members on page 371).
More information	Use this button to show the legend that explains the content of the overview (see Displaying role memberships of my resources' members on page 371).

Assignment resources (page description)

To open the **Assignment resources** page go to **Responsibilities** > **My Responsibilities** > **Assignment resources**.

On the **Assignment resources** page, you can see all the assignment resources that you manage (see Displaying my assignment resources on page 451).

If you click an assignment resource in the list, a new page opens (see Assignment resource overview page (page description) on page 1137), which contains more information and configuration options for the assignment resource.

The following tables give you an overview of the different functions and content on the **Assignment resources** page.

Table 444: Columns

Column	Description
Name	Shows the assignment resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Assignment resource overview page (page description)

To open an assignment resource's overview page go to **Responsibilities** > **My Responsibilities** > **Assignment resources** and click an assignment resource.

On the assignment resource's overview page, you can perform various actions on the assignment resource you selected beforehand.

To do this, click on one of the tiles:

Table 445: Tiles

Tile	Description
Overview	Opens the **Overview - Assignment resource** page (see Overview – Assignment resource (page description) on page 1138). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my assignment resource overviews on page 451). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Assignment resource** page (see Main data – Assignment resource (page description) on page 1138). Here you can see and edit the assignment resource's main data (see Displaying and editing my assignment resource main data on page 452).
Attestation	Opens the **Attestation – Assignment resource** page (see Attestation - Assignment resource (page description) on page 1139). You select the following actions: • Display all attestation cases linked to this assignment resource (see Displaying my assignment resource pending attestation cases on page 453) • Display details of the objects being attested (see Displaying my assignment resource pending attestation cases on page 453) • Make approval decisions about pending attestation cases (see Approving and denying my assignment resource attestation cases on page 455) • Display attestors of pending attestation cases (seeDisplaying attestors of my assignment resource pending attestation cases on

Tile	Description
	page 454) • Send reminders to approvers (see Sending reminders about my assignment resource pending attestation cases on page 456)

Overview – Assignment resource (page description)

To open the **Overview – Assignment resource** page go to **Responsibilities** > **My Responsibilities** > **Assignment resources** > select assignment resource > **Overview**.

On the **Overview - Assignment resource** page, you can see all the information relevant to the assignment resource summarized in an overview (see Displaying my assignment resource overviews on page 451).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Assignment resource (page description)

To open the **Main data – Assignment resource** page go to **Responsibilities** > **My Responsibilities** > **Assignment resources** > select assignment resource > **Main data**.

On the **Main data - Assignment resource** page, you can show and edit the assignment resource's main data (see Displaying and editing my assignment resource main data on page 452).

The following tables give you an overview of the different functions and content on the **Main data – Assignment resource** page.

Table 446: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 447: Assignment resource main data

Property	Description
Assignment resource	Enter a full, descriptive name for the assignment resource.
Resource type	Select the resource type of the assignment resource. Use resource types to group assignment resources.
Description	Enter a full, descriptive name for the assignments resource.
IT shop	Shows whether the assignment resource can be requested through the IT Shop. The assignment resource can be requested by its identities

Property	Description
	through the Web Portal and distributed using a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*. This option cannot be disabled.
Only use in IT Shop	Shows whether the assignment resource can only be requested through the IT Shop. The assignment resource can be requested by its identities through the Web Portal and distributed using a defined approval process. You cannot assign an assignment resource to hierarchical roles directly. This option cannot be disabled.
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use an assignment resource until a service item has been assigned to it.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning assignment resources to identities. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
Requested assignments remain intact.	Select the check box to convert assignments to roles into direct assign-ments if the request recipient is removed from the customer node of the associated shop. The option can only be edited as long as there is a request has not been assigned with this assignment resource.

Attestation - Assignment resource (page description)

To open the **Attestation – Assignment resource** page go to **Responsibilities** > **My Responsibilities** > **Assignment resources** > select assignment resource > **Attestation**.

On the **Attestation – Assignment resource** page, you can:

- Display all attestation cases linked to this assignment resource (see Displaying my assignment resource pending attestation cases on page 453)
- Display details of the objects being attested (see Displaying my assignment resource pending attestation cases on page 453)
- Make approval decisions about pending attestation cases (see Approving and denying my assignment resource attestation cases on page 455)
- Display attestors of pending attestation cases (seeDisplaying attestors of my assignment resource pending attestation cases on page 454)

- Send reminders to approvers (see Sending reminders about my assignment resource pending attestation cases on page 456)

The following tables give you an overview of the various features and content on the **Attestation – Assignment resource** page.

Table 448: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my assignment resource pending attestation cases on page 454). Then you can send reminder emails to these identities (see Sending reminders about my assignment resource pending attestation cases on page 456).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my assignment resource pending attestation cases on page 456).
Approve	Opens the **Pending Attestations – Assignment resources** page (see Pending attestations – Assignment resource (page description) on page 951). Use this button to make approval decisions about attestation cases pending for the assignment resource (see Displaying attestors of my assignment resource pending attestation cases on page 454).

Table 449: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my assignment resource pending attestation cases on page 454). Then you can send reminder emails to these identities (see Sending reminders about my assignment resource pending attestation cases on page 456).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my assignment resource pending attestation cases on page 453).

Table 450: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation	Shows the name of the attestation policy in use.

Column	Description
policy	
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Multi-request resources (page description)

To open the **Multi-request resources** page go to **Responsibilities** > **My Responsibilities** > **Multi-request resources**.

On the **Multi-request resources** page, you can see all the multi-request resources that you manage (see Displaying my multi-request resources on page 342).

If you click a multi-request resource in the list, a new page opens (see Multi-request resource overview page (page description) on page 1142), which contains more information and configuration options for the multi-request resource.

The following tables give you an overview of the different functions and content on the **Multi-request resources** page.

Table 451: Columns

Column	Description
Name	Shows the multi-request resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Multi-request resource overview page (page description)

To open a multi-request resource's overview page go to **Responsibilities** > **My Responsibilities** > **Multi-request resources** and click a multi-request resource.

On the multi-request resource's overview page, you can perform various actions on the multi-request resource you selected beforehand.

To do this, click on one of the tiles:

Table 452: Tiles

Tile	Description
Overview	Opens the **Overview - Multi-request resource** page (see Overview – Multi-request resource (page description) on page 1142). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my multi-request resources' overviews on page 343). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Multi-request resource** page (see Main data – Multi-request resource (page description) on page 1143). Here you can see and edit the multi-request resource's main data (see Displaying and editing my multi-request resources' main data on page 343).
Attestation	Opens the **Attestations – Multi-request resource** (see Attestation – Multi-request resource (page description) on page 1144). You select the following actions: • Display all attestation cases linked to this multi-request resource (see Displaying my multi-request resources' attestation cases on page 345) • Display details of the objects being attested (see Displaying my multi-request resources' attestation cases on page 345) • Make approval decisions about pending attestation cases (see Approving and denying my multi-request resources' attestation cases on page 347) • Display attestors of pending attestation cases (see Displaying attestors of my multi-request resources' pending attestation cases on page 346) • Send reminders to approvers (see Sending reminders about my multi-request resources' pending attestation cases on page 348)

Overview – Multi-request resource (page description)

To open the **Overview – Multi-request resource** page go to **Responsibilities** > **My Responsibilities** > **Multi-request resources** > select multi-request resource >

Overview.

On the **Overview – Multi-request resource** page, you can see all the information relevant to the multi-request resource summarized in an overview (see Displaying my multi-request resources' overviews on page 343).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Multi-request resource (page description)

To open the **Main data – Multi-request resource** page go to **Responsibilities** > **My Responsibilities** > **Multi-request resources** > select multi-request resource > **Main data**.

On the **Main data - Multi-request resource** page, you can show and edit the multi-request resource's main data (see Displaying and editing my multi-request resources' main data on page 343).

The following tables give you an overview of the different functions and content on the **Main data – Multi-request resource** page.

Table 453: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 454: Multi-request resource main data

Property	Description
Multi-request resource	Enter a full, descriptive name for the multi-request resource.
Resource type	Select the resource type of the multi-request resource. Use resource types to group multi-request resources.
Description	Enter a description for the multi-request resource.
IT Shop	Select the check box if the multi-request resource can also be requested through the IT Shop. This multi-request resource can be requested by your identities using the Web Portal and granted through a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the multi-request resource can only be requested through the IT Shop. This multi-request resource can be requested by your identities using the Web Portal and granted through a defined approval process. It is not possible to assign a multi-request resource

Property	Description
	directly to roles outside of the IT Shop (for example in the Manager).
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use an multi-request resource until a service item has been assigned to it.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning multi-request resources to identities. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Attestation – Multi-request resource (page description)

To open the **Attestation – Multi-request resource** page go to **Responsibilities** > **My Responsibilities** > **Multi-request resources** > select multi-request resource > **Attestation**.

On the **Attestation – Multi-request resource** page, you can:

- Display all attestation cases linked to this multi-request resource (see Displaying my multi-request resources' attestation cases on page 345)
- Display details of the objects being attested (see Displaying my multi-request resources' attestation cases on page 345)
- Make approval decisions about pending attestation cases (see Approving and denying my multi-request resources' attestation cases on page 347)
- Display attestors of pending attestation cases (see Displaying attestors of my multi-request resources' pending attestation cases on page 346)
- Send reminders to approvers (see Sending reminders about my multi-request resources' pending attestation cases on page 348)

The following tables give you an overview of the various features and content on the **Attestation – Multi-request resource** page.

Table 455: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my multi-request resources' pending attestation cases on page 346). Then you can send reminder emails to these identities (see Sending reminders about my multi-request resources' pending attestation cases on page 348).

Control	Description
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my multi-request resources' pending attestation cases on page 348).
Approve	Opens the **Pending Attestations – Multi-request resources** page (see Pending attestation – Multi-request resource (page description) on page 955). Use this button to make approval decisions about attestation cases pending for the multi-request resource (see Approving and denying my multi-request resources' attestation cases on page 347).

Table 456: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my multi-request resources' pending attestation cases on page 346). Then you can send reminder emails to these identities (see Sending reminders about my multi-request resources' pending attestation cases on page 348).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my multi-request resources' attestation cases on page 345).

Table 457: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.

Column	Description
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Software (page description)

To open the **Software** page go to **Responsibilities** > **My Responsibilities** > **Software**.

On the **Software** page, you can:

- View all the software applications that you manage (see Displaying my software applications on page 373)
- Create new software applications (see Adding your own software on page 373)

If you click a software application in the list, a new page opens (see Software application overview page (page description) on page 1148), which contains more information and configuration options for the software application.

The following tables give you an overview of the different functions and content on the **Software** page.

Table 458: Controls

Control	Description
New software	Opens the **New software** page (see New software (page description) on page 1147). Use this button to add a new software to the system (see Adding your own software on page 373).

Table 459: Columns

Column	Description
Name	Shows the software application's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

New software (page description)

To open the **New software** page go to **Responsibilities** > **My Responsibilities** > **System Roles** > **New software**.

On the **New software** page, you can create a new software application for which you are responsible. Do this by entering the new software application's main data (see Adding your own software on page 373).

Enter the following main data.

Table 460: Software application main data

Property	Description
Software name	Enter a full, descriptive name for the software application.
Version	Enter the version of the software application.
Language	Click **Assign**/**Change** and select the software application's language.
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use a software application until a service item has been assigned to it.
Internal product name	Enter a company internal name for the software application.
Website.	Enter the URL of the manufacturer's product website.
Link to documentation	Enter the URL of the documentation website.
Description	Enter a description for the software application.
Comment	Enter a comment for the software application.
IT shop	Select the check box if the software application can be requested through the IT Shop. This software application can be requested by identities using the Web Portal and granted through a defined approval process. The software application can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the software application can only requested through the IT Shop. This software application can be requested by identities using the Web Portal and granted through a defined approval process. The software may not be assigned directly to hierarchical roles.
Disabled	Select the check box if the software application is not used. Only

Property	Description
	enabled software applications can be assigned in One Identity Manager. If a software application is disabled, the software cannot be assigned but any existing assignments are upheld.

Software application overview page (page description)

To open a software application's overview page go to **Responsibilities** > **My Responsibilities** > **Software** and click a software application.

On the software's overview page, you can perform various actions on the software you selected beforehand.

To do this, click on one of the tiles:

Table 461: Tiles

Tile	Description
Overview	Opens the **Overview - Software** page (see Overview - Software (page description) on page 1149). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my software applications' overviews on page 373). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data – Software** page (see Main data - Software (page description) on page 1149). Here you can see and edit the software's main data (see Displaying and editing my software applications' main data on page 374).
Memberships	Opens the **Memberships – Software** page (see Memberships – Software (page description) on page 1150). You select the following actions: • Display identities that are assigned this software application (see Displaying memberships in my software applications on page 375) • Request the software application for identities (see Assigning identities to my software applications on page 375) • Cancel the software application for identities (seeRemoving identities from my software applications on page 376)
Attestation	Opens the **Attestations – Software** (see Attestation – Software (page description) on page 1152). You select the following actions: • Display all attestation cases linked to this software application (see Displaying my software applications' attestation cases on

Tile	Description
	page 377) • Display details of the objects being attested (see Displaying my software applications' attestation cases on page 377) • Make approval decisions about pending attestation cases (see Approving and denying my software applications' attestation cases on page 380) • Display attestors of pending attestation cases (see Displaying attestors of my software applications' pending attestation cases on page 379) • Send reminders to approvers (see Sending reminders about my software applications' pending attestation cases on page 381)
Usage	Opens the **Usage – Software** page (see Usage – Software (page description) on page 1153). Here you can see which roles and organizations belong to members of the software application (see Displaying role memberships of my software applications' members on page 383).

Overview - Software (page description)

To open the **Overview – Software** page go to **Responsibilities** > **My Responsibilities** > **Software** > select software > **Overview**.

On the **Overview – Software** page, you can see all the information relevant to the software application summarized in an overview (see Displaying my software applications' overviews on page 373).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data - Software (page description)

To open the **Main data – Software** page go to **Responsibilities** > **My Responsibilities** > **Software** > select software > **Main data**.

On the **Main data - Software** page, you can show and edit the software's main data (see Displaying and editing my software applications' main data on page 374).

The following tables give you an overview of the different functions and content on the **Main data – Software** page.

Table 462: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 463: Software application main data

Property	Description
Software name	Enter a full, descriptive name for the software application.
Version	Enter the version of the software application.
Language	Click **Assign**/**Change** and select the software application's language.
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use a software application until a service item has been assigned to it.
Internal product name	Enter a company internal name for the software application.
Website.	Enter the URL of the manufacturer's product website.
Link to documentation	Enter the URL of the documentation website.
Description	Enter a description for the software application.
Comment	Enter a comment for the software application.
IT shop	Select the check box if the software application can be requested through the IT Shop. This software application can be requested by identities using the Web Portal and granted through a defined approval process. The software application can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the software application can only requested through the IT Shop. This software application can be requested by identities using the Web Portal and granted through a defined approval process. The software may not be assigned directly to hierarchical roles.
Disabled	Select the check box if the software application is not used. Only enabled software applications can be assigned in One Identity Manager. If a software application is disabled, the software cannot be assigned but any existing assignments are upheld.

Memberships – Software (page description)

To open the **Memberships – Software** page go to **Responsibilities** > **My Responsibilities** > **Software** > select software > **Memberships**.

On the **Memberships - Software** page, you can:

- Display identities that are assigned this software application (see Displaying memberships in my software applications on page 375)
- Request the software application for identities (see Assigning identities to my software applications on page 375)
- Cancel the software application for identities (seeRemoving identities from my software applications on page 376)

The following tables give you an overview of the different functions and content on the **Memberships – Software** page.

Table 464: Controls

Control	Description
Request memberships	Use this button to request the software application for identities (see Assigning identities to my software applications on page 375).
Deleting memberships	Use this button to delete software application's assignment for selected identities (see Removing identities from my software applications on page 376). Select the check boxes in front of the identities whose software assignments you want to delete and click this button.

Table 465: Columns

Column	Description
Identity	Shows you the name of the identity to which the software application is assigned.
Origin	Shows you whether the software application was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Software (page description)

To open the **Attestation – Software** page go to **Responsibilities** > **My Responsibilities** > **Software** > select software > **Attestation**.

On the **Attestation – Software** page, you can:

- Display all attestation cases linked to this software application (see Displaying my software applications' attestation cases on page 377)
- Display details of the objects being attested (see Displaying my software applications' attestation cases on page 377)
- Make approval decisions about pending attestation cases (see Approving and denying my software applications' attestation cases on page 380)
- Display attestors of pending attestation cases (see Displaying attestors of my software applications' pending attestation cases on page 379)
- Send reminders to approvers (see Sending reminders about my software applications' pending attestation cases on page 381)

The following tables give you an overview of the various features and content on the **Attestation – Software** page.

Table 466: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my software applications' pending attestation cases on page 379). Then you can send reminder emails to these identities (see Sending reminders about my software applications' pending attestation cases on page 381).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my software applications' pending attestation cases on page 381).
Approve	Opens the **Pending Attestations – Software** page (see Pending attestations – Software (page description) on page 959). Use this button to make approval decisions about attestation cases pending for the software application (see Approving and denying my software applications' attestation cases on page 380).

Table 467: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my software applications' pending attestation cases on page 379). Then

Control	Description
	you can send reminder emails to these identities (see Sending reminders about my software applications' pending attestation cases on page 381).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my software applications' attestation cases on page 377).

Table 468: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Software (page description)

To open the **Usage – Software** page go to **Responsibilities** > **My Responsibilities** > **Software** > select software > **Usage**.

On the **Usage – Software** page, you can see the roles and organizations that belong to the identities to which this software application is assigned (see Displaying role memberships of my software applications' members on page 383).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the various features on the **Usage – Software** page.

Table 469: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to see (see Displaying role memberships of my software applications' members on page 383).
More information	Use this button to show the legend that explains the content of the overview (see Displaying role memberships of my software applications' members on page 383).

Multi requestable/unsubscribable resources (page description)

To open the **Multi requestable/unsubscribable resources** page go to **Responsibilities** > **My Responsibilities** > **Multi requestable/unsubscribable resources**.

On the **Multi requestable/unsubscribable resources** page, you can see all the multi requestable/unsubscribable resources that you manage (see Displaying my multi requestable/unsubscribable resources on page 350).

If you click a multi requestable/unsubscribable resource in the list, a new page opens (see Multi requestable/unsubscribable resource overview page (page description) on page 1154), which contains more information and configuration options for the multi requestable/unsubscribable resource.

The following tables give you an overview of the different functions and content on the **Multi requestable/unsubscribable resources** page.

Table 470: Columns

Column	Description
Name	Shows the multi requestable/unsubscribable resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Multi requestable/unsubscribable resource overview page (page description)

To open a multi requestable/unsubscribable resource's overview page go to **Responsibilities** > **My Responsibilities** > **Multi requestable/unsubscribable Resources** and click a multi requestable/unsubscribable resource.

On the multi requestable/unsubscribable resource's overview page, you can perform various actions on the multi requestable/unsubscribable resource you selected beforehand.

To do this, click on one of the tiles:

Table 471: Tiles

Tile	Description
Overview	Opens the **Overview - Multi requestable/unsubscribable resource** page (see Overview – Multi requestable/unsubscribable resource (page description) on page 1156). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my multi requestable/unsubscribable resources' overviews on page 351). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Multi requestable/unsubscribable resource** page (see Main data – Multi requestable/unsubscribable resource (page description) on page 1156). Here you can see and edit the multi requestable/unsubscribable resource's main data (see Managing my multi requestable/unsubscribable resources on page 350).
Memberships	Opens the **Memberships – Multi requestable/unsubscribable resource** page (see Memberships – Multi requestable/unsubscribable resource (page description) on page 1158). You select the following actions: • Display identities that are assigned this multi requestable/unsubscribable resource (see Displaying my multi requestable/unsubscribable resources' memberships on page 353) • Request this multi requestable/unsubscribable resource for identities (see Assigning identities to my multi requestable/unsubscribable resources on page 353) • Cancel this multi requestable/unsubscribable resource for identities (see Removing identities from my multi requestable/unsubscribable resources on page 354)
Attestation	Opens the **Attestations – Multi requestable/unsubscribable resource** page (see Attestation – Multi requestable/unsubscribable resource (page description) on page 1159). Opens the **Attestation – Device** page (see Attestations – Device (page description) on page 1168). You select the following actions: • Display all attestation cases linked to this multi requestable/unsubscribable resource (see Displaying my multi

Tile	Description
	requestable/unsubscribable resources' attestation cases on page 356) • Display details of the objects being attested (see Displaying my multi requestable/unsubscribable resources' attestation cases on page 356) • Make approval decisions about pending attestation cases (see Approving and denying my multi requestable/unsubscribable resources' attestation cases on page 358) • Display attestors of pending attestation cases (see Displaying attestors of my multi requestable/unsubscribable resources' pending attestation cases on page 357) • Send reminders to approvers (see Sending reminders about my multi requestable/unsubscribable resources' pending attestation cases on page 359)

Overview – Multi requestable/unsubscribable resource (page description)

To open the **Overview – Multi requestable/unsubscribable resource** page go to **Responsibilities** > **My Responsibilities** > **Multi requestable/unsubscribable** > select Multi requestable/unsubscribable resource > **Overview**.

On the **Overview – Multi requestable/unsubscribable resource** page, you can see all the information relevant to the multi requestable/unsubscribable resource summarized in an overview (see Displaying my multi requestable/unsubscribable resources' overviews on page 351).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Multi requestable/unsubscribable resource (page description)

To open the **Main data – Multi requestable/unsubscribable resource** page go to **Responsibilities** > **My Responsibilities** > **Multi requestable/unsubscribable** > select multi requestable/unsubscribable resource > **Main data**.

On the **Main data - Multi requestable/unsubscribable resource** page, you can show and edit the ulti requestable/unsubscribable resource's main data (see Displaying and editing my multi requestable/unsubscribable resources' main data on page 351).

The following tables give you an overview of the different functions and content on the **Main data – Multi requestable/unsubscribable resource** page.

Table 472: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 473: Multi requestable/unsubscribable resource main data

Property	Description
Multi requestable/unsubscribable resource	Enter a full, descriptive name for the multi requestable/unsubscribable resource.
Resource type	Select the resource type of the multi requestable/un-subscribable resource. Use resource types to group multi requestable/un-subscribable resources.
Description	Enter a description for the multi requestable/un-subscribable resource.
IT shop	Select the check box if the multi requestable/unsubscribable resource can also be requested through the IT Shop. This multi requestable/unsubscribable resource can be requested by your identities using the Web Portal and granted through a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the multi requestable/un-subscribable resource can only be requested through the IT Shop. This multi requestable/unsubscribable resource can be requested by your identities using the Web Portal and granted through a defined approval process. It is not possible to assign a multi requestable/unsubscribable resource directly to roles outside of the IT Shop (for example in the Manager).
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use an multi requestable/unsubscribable resource until a service item has been assigned to it.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning multi requestable/un-subscribable resources to identities. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Memberships – Multi requestable/unsubscribable resource (page description)

To open the **Memberships – Multi requestable/unsubscribable resource** page go to **Responsibilities** > **My Responsibilities** > **Multi requestable/unsubscribable** > select Multi requestable/unsubscribable resource > **Memberships**.

On the **Memberships - Multi requestable/unsubscribable resource** page, you can:

- Display identities that are assigned this multi requestable/unsubscribable resource (see Displaying my multi requestable/unsubscribable resources' memberships on page 353)
- Request this multi requestable/unsubscribable resource for identities (see Assigning identities to my multi requestable/unsubscribable resources on page 353)
- Cancel this multi requestable/unsubscribable resource for identities (see Removing identities from my multi requestable/unsubscribable resources on page 354)

The following tables give you an overview of the different functions and content on the **Attestation – Multi requestable/unsubscribable resource** page.

Table 474: Controls

Control	Description
Request memberships	Use this button to request the multi-request resource for identities (see Assigning identities to my multi requestable/unsubscribable resources on page 353).
Deleting memberships	You can use this button to delete the assignment of the multi requestable/unsubscribable resource for selected identities (see Removing identities from my multi requestable/unsubscribable resources on page 354). Select the check boxes in front of the identities whose multi requestable/unsubscribable resources you want to delete and click this button.

Table 475: Columns

Column	Description
Identity	Shows you the name of the identity to which the multi requestable/unsubscribable resource is assigned.
Origin	Shows you whether the multi requestable/unsubscribable resource was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Multi requestable/unsubscribable resource (page description)

To open the **Attestation – Multi requestable/unsubscribable resource** page go to **Responsibilities** > **My Responsibilities** > **Multi requestable/unsubscribable** > select Multi requestable/unsubscribable resource > **Attestation**.

On the **Attestation – Multi requestable/unsubscribable resource** page, you can:

- Display all attestation cases linked to this multi requestable/unsubscribable resource (see Displaying my multi requestable/unsubscribable resources' attestation cases on page 356)
- Display details of the objects being attested (see Displaying my multi requestable/unsubscribable resources' attestation cases on page 356)
- Make approval decisions about pending attestation cases (see Approving and denying my multi requestable/unsubscribable resources' attestation cases on page 358)
- Display attestors of pending attestation cases (see Displaying attestors of my multi requestable/unsubscribable resources' pending attestation cases on page 357)
- Send reminders to approvers (see Sending reminders about my multi requestable/unsubscribable resources' pending attestation cases on page 359)

The following tables give you an overview of the various features and content on the **Attestation – Multi requestable/unsubscribable resource** page.

Table 476: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my multi requestable/unsubscribable resources' pending attestation cases on page 357). Then you can send reminder emails to these identities (see Sending reminders about my multi requestable/unsubscribable resources' pending attestation cases on page 359).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending

Control	Description
	reminders about my multi requestable/unsubscribable resources' pending attestation cases on page 359).
Approve	Opens the **Pending Attestations – Multi requestable/un-subscribable resources** page (see Pending attestations – Multi requestable/unsubscribable resource (page description) on page 963). Use this button to make approval decisions about attestation cases pending for the multi requestable/unsubscribable resource (see Approving and denying my multi requestable/unsubscribable resources' attestation cases on page 358).

Table 477: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my multi requestable/unsubscribable resources' pending attestation cases on page 357). Then you can send reminder emails to these identities (see Sending reminders about my multi requestable/unsubscribable resources' pending attestation cases on page 359).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my multi requestable/unsubscribable resources' attestation cases on page 356).

Table 478: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied

Column	Description
	approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Devices (page description)

To open the **Devices** page go to **Responsibilities** > **My Responsibilities** > **Devices**.

On the **Devices** page, you can:

- View all the devices that you manage (see Displaying my devices on page 262)
- Add new devices (see Adding your own devices on page 262)

If you click a device in the list, a new page opens (see Device overview page (page description) on page 1164), which contains more information and configuration options for the device.

The following tables give you an overview of the different functions and content on the **Devices** page.

Table 479: Controls

Control	Description
Adding new devices	Open the **Add new device** page (see Adding new devices (page description) on page 1162). Use this button to add a new device to the system (see Adding your own devices on page 262).

Table 480: Columns

Column	Description
Display	Shows the device's name.
Device model	Shows the model of the device.
Used by	Shows which identities use the device.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Adding new devices (page description)

To open the **Add a new device** page go to **Responsibilities** > **My Responsibilities** > **Device** > **Add a new device**.

On the **Add a new device** page, you can create a new device for which you are responsible. Do this by entering the new device's main data (see Adding your own devices on page 262).

Enter the following main data.

Table 481: Mobile phone main data

Property	Description
Device type	In the menu, select the type of device.
Used by	Click **Change** and select the identity that will use the device.
Device model	Click **Assign/Change** and select the device's model.
Manufacturer	Click **Assign/Change** and select the manufacturer of the device.
Device ID	Enter a name for the device.
Device status	Click **Assign/Change** and select the device's status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
Storage capacity [GB]	Enter the device's storage capacity (in gigabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.
Asset number	Enter the device's asset number.
Company owned	Select the check box if the device belongs to the company.

Table 482: PC main data

Property	Description
Device type	In the menu, select the type of device.
Used by	Click **Change** and select the identity that will use the device.
Device model	Click **Assign**/**Change** and select the device's model.
Manufacturer	Click **Assign**/**Change** and select the manufacturer of the device.
Device ID	Enter a name for the device.
Device status	Click **Assign**/**Change** and select the device's status.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
Storage capacity [GB]	Enter the device's storage capacity (in gigabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
MAC address	Enter the device's MAC address.
PC	Select the check box if this is a simple desktop PC for an identity.
Servers	Select the check box if this is a server.
VM Host	Select the check box if this is a host for a virtual machine.
VM Client	Select the check box if this is a virtual machine.
VM Host	Click **Assign**/**Change** and select the device you want to install the virtual machine on. The select is available if the **VM Client** check box is set.
MAC address	Enter the device's MAC address.
Asset number	Enter the device's asset number.
Company owned	Select the check box if the device belongs to the company.

Table 483: Tablet main data

Property	Description
Device type	In the menu, select the type of device.
Used by	Click **Change** and select the identity that will use the device.

Property	Description
Device model	Click **Assign**/**Change** and select the device's model.
Manufacturer	Click **Assign**/**Change** and select the manufacturer of the device.
Device ID	Enter a name for the device.
Device status	Click **Assign**/**Change** and select the device's status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
Storage capacity [GB]	Enter the device's storage capacity (in gigabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.
Asset number	Enter the number of the asset in the device's bookkeeping.
Company owned	Select the check box if the device belongs to the company.

Device overview page (page description)

To open a device's overview page go to **Responsibilities** > **My Responsibilities** > **Devices** and click a device.

On the device's overview page, you can perform various actions on the device you selected.

To do this, click on one of the tiles:

Table 484: Tiles

Tile	Description
Overview	Opens the **Overview - Device** page (see Overview – Device (page description) on page 1165). Here you can see all the relevant information about departments summarized in an overview. (see Displaying my devices' overviews on page 263). For more information, click on the links inside one of the

Tile	Description
	shapes.
Main data	Opens the **Main data - Device** page (see Main data – Device (page description) on page 1165). Here you can see and edit the device's main data (see Displaying and editing my devices' main data on page 263).
Attestation	You select the following actions: • Display all attestation cases linked to this device (see Displaying my devices' attestation cases on page 265) • Display details of the objects being attested (see Displaying my devices' attestation cases on page 265) • Make approval decisions about pending attestation cases (see Approving and denying my devices' attestation cases on page 267) • Display attestors of pending attestation cases (see Displaying attestors of my devices' pending attestation cases on page 266) • Send reminders to approvers (see Sending reminders about my devices' pending attestation cases on page 268)

Overview – Device (page description)

To open the **Overview – Device** page go to **Responsibilities** > **My Responsibilities** > **Device** > select device > **Overview**.

On the **Overview - Device** page, you can see all the information relevant to the device summarized in an overview (see Displaying my devices' overviews on page 263).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Device (page description)

To open the **Main data – Device** page go to **Responsibilities** > **My Responsibilities** > **Device** > select device > **Main data**.

On the **Main data - Device** page, you can show and edit the device's main data (see Displaying and editing my devices' main data on page 263).

The following tables give you an overview of the different functions and content on the **Main data – Device** page.

Table 485: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 486: Mobile phone main data

Property	Description
Device type	In the menu, select the type of device.
Used by	Click **Change** and select the identity that will use the device.
Device model	Click **Assign**/**Change** and select the device's model.
Manufacturer	Click **Assign**/**Change** and select the manufacturer of the device.
Device ID	Enter a name for the device.
Device status	Click **Assign**/**Change** and select the device's status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
Storage capacity [GB]	Enter the device's storage capacity (in gigabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.
Asset number	Enter the device's asset number.
Company owned	Select the check box if the device belongs to the company.

Table 487: PC main data

Property	Description
Device type	In the menu, select the type of device.
Used by	Click **Change** and select the identity that will use the device.
Device model	Click **Assign**/**Change** and select the device's model.
Manufacturer	Click **Assign**/**Change** and select the manufacturer of the device.
Device ID	Enter a name for the device.
Device status	Click **Assign**/**Change** and select the device's status.

Property	Description
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
Storage capacity [GB]	Enter the device's storage capacity (in gigabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
MAC address	Enter the device's MAC address.
PC	Select the check box if this is a simple desktop PC for an identity.
Servers	Select the check box if this is a server.
VM Host	Select the check box if this is a host for a virtual machine.
VM Client	Select the check box if this is a virtual machine.
VM Host	Click **Assign**/**Change** and select the device you want to install the virtual machine on. The select is available if the **VM Client** check box is set.
MAC address	Enter the device's MAC address.
Asset number	Enter the device's asset number.
Company owned	Select the check box if the device belongs to the company.

Table 488: Tablet main data

Property	Description
Device type	In the menu, select the type of device.
Used by	Click **Change** and select the identity that will use the device.
Device model	Click **Assign**/**Change** and select the device's model.
Manufacturer	Click **Assign**/**Change** and select the manufacturer of the device.
Device ID	Enter a name for the device.
Device status	Click **Assign**/**Change** and select the device's status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.

Property	Description
Serial number	Enter the device's serial number.
Storage capacity [GB]	Enter the device's storage capacity (in gigabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.
Asset number	Enter the number of the asset in the device's bookkeeping.
Company owned	Select the check box if the device belongs to the company.

Attestations – Device (page description)

To open the **Attestation – Device** page go to **Responsibilities** > **My Responsibilities** > **Devices** > select device > **Attestation**.

On the **Attestation - Device** page, you can:

- Display all attestation cases linked to this device (see Displaying my devices' attestation cases on page 265)
- Display details of the objects being attested (see Displaying my devices' attestation cases on page 265)
- Make approval decisions about pending attestation cases (see Approving and denying my devices' attestation cases on page 267)
- Display attestors of pending attestation cases (see Displaying attestors of my devices' pending attestation cases on page 266)
- Send reminders to approvers (see Sending reminders about my devices' pending attestation cases on page 268)

The following tables give you an overview of the various features and content on the **Attestations - Device** page.

Table 489: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of my devices' pending attestation cases on page 266). Then you can send reminder emails to these identities (see Sending reminders about my

Control	Description
	devices' pending attestation cases on page 268).
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about my devices' pending attestation cases on page 268).
Approve	Opens the **Pending Attestations – Device** page (see Pending attestations: Device (page description) on page 966). Use this button to make approval decisions about attestation cases pending for the device (see Approving and denying my devices' attestation cases on page 267).

Table 490: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of my devices' pending attestation cases on page 266). Then you can send reminder emails to these identities (see Sending reminders about my devices' pending attestation cases on page 268).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying my devices' attestation cases on page 265).

Table 491: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been

Column	Description
	granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Delegating tasks (page description)

To open the **Delegation** page go to **Responsibilities** > **Delegation**.

On the **Delegation** page you can perform various actions regarding the delegation of role memberships and responsibilities.

To do this, click on one of the tiles:

Table 492: Tiles

Tiles	Description
Deleg- ation	You select the following actions: • Display delegations created by you or by others for you (see Displaying delegations on page 458) • Delegate role memberships and responsibilities (see Creating delegations on page 459) • Cancel delegations (see Deleting my identities' delegations on page 308) • Delete delegations (see Deleting my identities' delegations on page 308)
Deleg- ation history	Here you can display past delegations you have been involved in (see Displaying delegation history on page 462).

Delegation (page description)

To open the **Delegation** page go to **Responsibilities** > **Delegation** > **Delegation**.

Delegations are responsibilities that you have assigned to other identities or that have been delegated to you.

On the **Delegation** page, you can:

- Display delegations created by you or by others for you (see Displaying delegations on page 458)
- Delegate role memberships and responsibilities (see Creating delegations on page 459)
- Cancel delegations (see Deleting my identities' delegations on page 308)
- Delete delegations (see Deleting my identities' delegations on page 308)

The following tables give you an overview of the various features and content on the **Delegation** page.

Table 493: Controls

Control	Description
Select	Use this button to select a delegation that you want to delete later using **Actions** > **Delete delegation** (see Deleting delegations on page 461).
Select all	Use this button to select all the delegations in the list so that you can delete them later using **Actions** > **Delete delegation** (see Deleting delegations on page 461).
Actions > Delete all my delegations	Use this action to delete all the delegation that you created yourself (see Deleting delegations on page 461).
Actions > Delete delegation	Use this action to delete all the delegations selected in the **Delete** column (see Deleting delegations on page 461).
Actions > Select all	Use this action to select all the delegations that you want to delete later using **Actions** > **Delete delegation** (see Deleting delegations on page 461).
New delegation	Use this button to transfer responsibility to another identity (see Creating delegations on page 459).

Table 494: Controls in the details pane of a delegation

Control	Description
Withdraw request	Use this button to withdraw the delegation of responsibility (see Canceling delegations on page 460). This is possible until the delegation is approved.
Delete	Use this button to delete the delegation (see Deleting delegations on page 461).
Details	You can use this button to display more information about the delegation, which is distributed over the following tabs (see Displaying delegations on page 458): NOTE: In the Web Portal, a delegation is treated like a request.

Control	Description
	• **Information**: Displays general information about a request. • **Workflow**: Displays the life cycle chronologically as from the time of request. • **Compliance**: Displays possible rule violations for this request. • **Entitlements**: Displays which entitlements are assigned to the delegated application role. This tab is only displayed if it is a delegation of an application role.

Table 495: Columns

Column	Description
Name	Shows you the name of the object whose responsibility has been delegated.
Delegator	Shows you the name of the identity that created the delegation.
Delegation recipient	Shows you the name of the identity to which the responsibility was delegated.
Assignment Method	Shows you what type of delegated responsibility it is. For example, if you delegate responsibility through an identity, the criteria is **Employee manager**.
Delete	Use the buttons to select delegations that you want to delete later using **Actions** > **Delete delegation**.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: You can view more information about each delegation on the tabs in the detail pane.

Delegation history (page description)

To open the **Delegation History** page go to **Responsibilities** > **Delegation** > **Delegation History**.

On the **Delegation History** page, you can display previous delegations that you were involved in (see Displaying delegation history on page 462).

If you want to display only delegations of a specific identity or delegated to a specific identity, use the advanced search.

The delegations are divided into different sections on the following tabs to provide a clearer overview:

- **Delegated to you**: Shows you responsibilities/role memberships that have been delegated to you.

- **Delegated to other identities**: Shows you responsibilities/role memberships that you have delegated to other identities.

The following tables give you an overview of the various features and content on the **Delegation History** page.

Table 496: Controls

Control	Description
Valid from	Use this option to cover all delegations that are valid from this time or from a time within this period.
Valid until	Use this option to cover all delegations that are valid until this time or until a time within this period.
Advanced search	The advanced search allows you to control which delegations are displayed: • **Delegator**: Click **Assign/Change** and then click the appropriate identity. Only responsibilities/role memberships delegated by this identity are displayed. The corresponding delegations are displayed in the **Delegated to you** tab. • **Delegator recipient**: Click **Assign/Change** and then click the appropriate identity. Only responsibilities/role memberships delegated to this identity are displayed. The corresponding delegations are displayed in the **Delegated to other identities** tab. • **Show never assigned delegations**: Select the check box if you also want to show delegations that were in effect(for example, delegations that were rejected).
Search	Use this button to search using your defined criteria.

Table 497: Columns

Column	Description
Name	Shows you the name of the object whose responsibility/role membership has been delegated.
Type	Shows you what type of delegated responsibility/role membership it is. For example, if you delegate responsibility/role membership through an identity, it is the **Responsible** assignment type.
Valid from	Show you from when the delegation was valid.
Valid until	Show you until when the delegation was valid.
Delegated to	Shows you the name of the identity to which the responsibility/role membership was delegated.
Delegation of	Shows you the name of the identity that created the delegation.

TIP: On the following tabs, you can show other useful information about each delegation in the pane. To do this, click the corresponding entry in the list.

- **Information**: Displays general information about the delegation.
- **Workflow**: Shows the chronological lifecycle of the delegation.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Displays which entitlements are assigned to the delegated application role. This tab is only displayed if it is a delegation of an application role.
- **Delegation**: Shows you general information about delegation.

Ownerships (page description)

To open the **Ownerships** page go to **Responsibilities** > **Ownerships**.

On the **Ownerships** page, you can assign new owners to objects or take responsibility for groups.

To do this, click on one of the tiles:

Table 498: Tiles

Tile	Description
Assign Ownership	Here you can assign ownership to a business object without an owner (see Assigning owners to devices on page 464 and Assigning owners to system entitlements on page 464).
Claim ownership	Here you can take responsibility for Active Directory groups without owners (see Claiming ownership of Active Directory groups on page 465).

Assigning owners (page description)

To open the **Assign Ownership** page go to **Responsibilities** > **Ownerships** > **Assign Ownership**.

On the **Assign Ownership** page, you can:

- Assign devices without owners to new owners (see Assigning owners to devices on page 464)
- Assign system entitlements without owners to new owners (see Assigning owners to system entitlements on page 464)

Click the appropriate tile to begin assigning a new owner to a device or system entitlement.

Claim ownership (page description)

To open the **Claim Ownership** page go to **Responsibilities** > **Ownerships** > **Claim Ownership**.

On the **Claim Ownership** page you can claim responsibility for Active Directory groups without owners (see Claiming ownership of Active Directory groups on page 465).

The following table give you an overview of the various features on the **Claim Ownership** page.

Table 499: Controls

Control	Description
Select a group	Click **Assign**/**Change** and then on the Active Directory group whose responsibility you want to claim.
Claim ownership	You can use this button to claim responsibility for the selected Active Directory group (see Claiming ownership of Active Directory groups on page 465).

Auditing (page description)

To open the **Auditing** page go to **Responsibilities** > **Auditing**.

On the **Auditing** page, you can display all objects with their detailed information.

To do this, click on one of the tiles:

- Departments
- Business roles
- Cost centers
- Multi-request resources
- Multi requestable/unsubscribable resources
- Identities
- One Identity Manager application roles
- Resources
- Software
- Locations
- System roles
- Assignment resources
- Active Directory
- Azure Active Directory

- Custom target systems
- Google Workspace
- Domino
- LDAP
- Oracle E-Business Suite
- Privileged Account Management
- SAP R/3
- Unix

Auditing – Departments (page description)

To open the **Auditing - Departments** page go to **Responsibilities** > **Auditing** > **Departments**.

On the **Auditing - Departments** page, you can see all requests (see Displaying all departments on page 467).

If you click **Show details** in a department's details pane, a new page opens (see Auditing - Roles and permissions: department (page description) on page 1177) that contains more information and configuration options for the department.

The following tables give you an overview of the various features and content on the **Auditing – Departments** page.

Table 500: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the departments they manage are shown (see Displaying all departments on page 467).

Table 501: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - Roles and entitlements: department** page (see Auditing - Roles and permissions: department (page description) on page 1177). Use this button to display more details about the department.

Table 502: Columns

Column	Description
Display	Shows the department's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: department (page description)

To open the **Auditing - Roles and entitlements: department** page go to **Responsibilities** > **Auditing** > **Departments** > **Show details**.

On the **Auditing - Roles and entitlements: department** page, you can access various information about the selected department.

To do this, click on one of the tiles:

Table 503: Tiles

Tile	Description
Overview	Opens the **Overview – Department** page (see Overview – Department (page description) on page 1178) This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying department overviews on page 467) .
Main data	Opens the **Main data – Department** page (see Main data – Department (page description) on page 1178). Here you see the department's main data (see Displaying department main data on page 468).
Memberships	Opens the **Memberships – Department** page (see Memberships – Department (page description) on page 1179). Here you can see the identities assigned to the department (see Displaying department memberships on page 469).
Entitlements	Opens the **Entitlements – Department** page (see Entitlements – Department (page description) on page 1180) Here you can see the entitlements assigned to the department (see Displaying department entitlements on page 469).
Attestation	Opens the **Attestation – Department** page (see Attestation – Department (page description) on page 1181). You select the following actions: • Display all attestation cases linked to this department (see Displaying department attestation cases on page 470) • Display identities that have yet to approve department attestation cases (see Displaying attestors of department pending attestation cases on page 472)

Tile	Description
	• Display details of the objects being attested (see Displaying department attestation cases on page 470)
Compliance	Opens the **Compliance – Department** page (see Compliance – Department (page description) on page 1182). Here you can show compliance rule violations that were caused by this department (see Displaying department rule violations on page 473).
Risk	Opens the **Risk – Department** page (see Risk – Department (page description) on page 1183) Here you can see the department's risk index (see Displaying department risk indexes on page 474). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – Department** page (see History – Department (page description) on page 1183) Here you can see all the changes made to the department (see Department history on page 474).
Usage	Opens the **Usage – Department** page (see Usage – Department (page description) on page 1185) Here you can see which roles and organizations belong to members of the department (see Displaying role memberships of department members on page 478)

Overview – Department (page description)

To open the **Overview – Department** page go to **Responsibilities** > **Auditing** > **Departments** > **Show details** > **Overview**.

On the **Overview – Department** page, you can see all the information relevant to the department summarized in an overview (see Displaying department overviews on page 467).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Department (page description)

To open the **Main data – Department** page go to **Responsibilities** > **Auditing** > **Departments** > **Show details** > **Main data**.

On the **Main data - Department** page, you can see and edit the department's main data (see Displaying department main data on page 468).

Enter the following main data:

Table 504: Department main data

Property	Description
Department	Shows the full, descriptive name of the department.
Short name	Shows the department's short name.
Object ID	Show the department's unique object ID. For example, the object ID is required in SAP systems for assigning identities to departments.
Location	Shows the location that the department is primarily assigned to.
Parent department	Shows the parent department of this department. If the department is at the root of a department hierarchy, the field is empty.
Attestors	Shows the attestor application role. Members of this application role can approve attestation cases for the department.
Cost center	Shows the cost center that the department is primarily assigned to.
Role approver	Shows the role approver. Members of the selected application role can approve requests for members of the department.
Role approver (IT)	Shows the IT application role approver. Members of the selected application role can approve requests for members of the department.
Manager	Shows the identity responsible for the department.
2nd Manager	Shows the identity acting as a deputy to the department's manager.
Description	Shows the department's description.

Memberships – Department (page description)

To open the **Memberships – Department** page go to **Responsibilities** > **Auditing** > **Departments** > **Show details** > **Memberships**.

On the **Memberships - Department** page, you can see identities assigned to the department (see Displaying department memberships on page 469).

The following table gives an overview of the different content on the **Memberships – Department** page.

Table 505: Columns

Column	Description
Identity	Shows you the name of the identity assigned to the department.
Origin	Shows you whether the department was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Department (page description)

To open the **Entitlements – Department** page go to **Responsibilities** > **Auditing** > **Departments** > **Show details** > **Entitlements** .

On the **Entitlements – Department** page, you can see entitlements assigned to the department (see Displaying department entitlements on page 469).

The following table gives you an overview of the different functions and content on the **Entitlements – application roles** page.

Table 506: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Department (page description)

To open the **Attestation – Department** page go to **Responsibilities** > **Auditing** > **Departments** > **Show details** > **Attestation**.

On the **Attestation - Department** page, you can:

- Display all attestation cases linked to this department (see Displaying department attestation cases on page 470)
- Display identities that have yet to approve department attestation cases (see Displaying attestors of department pending attestation cases on page 472)
- Display details of the objects being attested (see Displaying department attestation cases on page 470)

The following tables give you an overview of the various features and content on the **Attestation - Department** page.

Table 507: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of department pending attestation cases on page 472).

Table 508: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying department attestation cases on page 470).

Table 509: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval.

Column	Description
	• **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Department (page description)

Open the **Compliance – Department** page by navigating through **Responsibilities** > **Auditing** > **Departments** > **Show details** > **Compliance**.

On the **Compliance – Department** page, you can see compliance rule violations connected with this department (see Displaying department rule violations on page 473).

The following table gives an overview of the content of the **Compliance – System role** page.

Table 510: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Department (page description)

Open the **Compliance – Department** page by navigating through **Responsibilities** > **Auditing** > **Departments** > **Show details** > **Compliance**.

On the **Risk – Department** page, you can:

- Display the department's calculated risk index (see Displaying department risk indexes on page 474)
- See how the calculated risk index is put together (see Displaying department risk indexes on page 474)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – Department** page.

Table 511: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying department risk indexes on page 474).

Table 512: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Department (page description)

To open the **History – Department** page go to **Responsibilities** > **Auditing** > **Departments** > **Show details** > **History**.

On the **History – Department** page, you can see all the changes made to the department (see Department history on page 474).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a department, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Department** page.

Table 513: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying department history on page 475). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying department history on page 475).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying department history on page 475).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of departments on page 477).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of departments on page 477).

Table 514: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of

Control	Description
	the property was at the selected point in time and what the value is now.

Table 515: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Department (page description)

To open the **Usage – Department** page go to **Responsibilities** > **Auditing** > **Departments** > **Show details** > **Usage**.

On the **Usage – Department** page, you can see the roles and organizations that belong to the identities to which this department is assigned (see Displaying role memberships of department members on page 478).

The following table gives you an overview of the various features on the **Usage – Departments** page.

Table 516: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Application roles (page description)

To open the **Auditing - One Identity Manager application roles** page go to **Responsibilities** > **Auditing** > **One Identity Manager application roles**.

On the **Auditing - One Identity Manager application roles** page, you can see all the application roles (see Displaying all application roles on page 479).

If you click **Show details** in an application role's details pane, a new page opens (see Auditing - Roles and entitlements: application role (page description) on page 1187) that contains more information and configuration options for the application role.

The following tables give you an overview of the various features and content on the **Auditing – One Identity Manager application roles** page.

Table 517: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the application roles they manage are shown (see Displaying all application roles on page 479).

Table 518: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: One Identity Manager application role** page (see Auditing - Roles and entitlements: application role (page description) on page 1187). Use this button to display more details about the application role.

Table 519: Columns

Column	Description
Display	Shows the application role's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and entitlements: application role (page description)

To open the **Auditing - Roles and entitlements: application role** page go to **Responsibilities** > **Auditing** > **One Identity Manager application roles** > **Show details**.

On the **Auditing - Roles and entitlements: application role** page, you can access various information about the selected application role.

To do this, click on one of the tiles:

Table 520: Tiles

Tile	Description
Overview	Opens the **Overview – Application role** page (see Overview – Application role (page description) on page 1188). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying application role overviews on page 479) .
Main data	Opens the **Main data – Application role** page (see Main data - Application role (page description) on page 1188).
Memberships	Opens the **Memberships – Application role** page (see Memberships – Application role (page description) on page 1189). Here you can see identities to which the application role is assigned (see Displaying memberships in application roles on page 481).
Entitlements	Opens the **Entitlements – Application role** page (see Entitlements – Application role (page description) on page 1190). Here you can see the entitlements assigned to the application role (see Displaying application role entitlements on page 481).
Attestation	Opens the **Attestation – Application role** page (see Attestation – Application role (page description) on page 1190). You select the following actions: • Display all attestation cases linked to this application role (see Displaying application role pending attestation cases on page 482)

Tile	Description
	• Display identities that have yet to approve application role attestation cases (see Displaying attestors of application role pending attestation cases on page 484) • Display details of the objects being attested (see Displaying application role pending attestation cases on page 482)
History	Opens the **History – Application role** page (see History – Application role (page description) on page 1192). Here you can see all the changes made to the application role (see Application role history on page 485).
Usage	Opens the **Usage – Application role** page (see Usage – Application role (page description) on page 1194). Here you can see which roles the members of the application role belong to (see Displaying role memberships of application role members on page 488).

Overview – Application role (page description)

To open the **Overview – Application role** page go to **Responsibilities** > **Auditing** > **Auditing - One Identity Manager application roles** > **Show details** > **Overview**.

On the **Overview – Application role** page, you can see all the information relevant to the application role summarized in an overview (see Displaying application role overviews on page 479).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data - Application role (page description)

To open the **Main data – Application Role** page go to **Responsibilities** > **Auditing** > **Auditing - One Identity Manager application roles** > **Show details** > **Main data**.

On the **Main data – Application role** page, you can see the application role's main data (see Displaying application role main data on page 480).

Enter the following main data:

Table 521: Application role main data

Property	Description
Application role	Shows the full, descriptive name of the application role.
Internal name	Shows the company internal name of the application role.

Property	Description
Location	Shows the location that the application role is primarily assigned to.
Parent application role	Shows the parent application role of this application role. If the application role is at the root of an application role hierarchy, the field is empty.
Department	Shows the department assigned to the application role.
Cost center	Shows the cost center that the application role is primarily assigned to.
Manager	Shows the identity responsible for the application role.
2nd Manager	Shows the identity acting as a deputy to the application role's manager.
Description	Show the application role's description.
Comment	Shows an informative comment about the application role.
Full name	Shows the full name of the application role, which is automatically made up of the identifiers of the application role and the parent application role.

Memberships – Application role (page description)

To open the **Memberships – Application role** page go to **Responsibilities** > **Auditing** > **Auditing - One Identity Manager application roles** > **Show details** > **Memberships**.

On the **Memberships - Application Role** page, you can see identities to which the application role is assigned (see Displaying memberships in application roles on page 481).

The following table gives an overview of the content on the **Memberships – Application role** page.

Table 522: Columns

Column	Description
Identity	Shows you the name of the identity to which the application role is assigned.
Origin	Shows you whether the application role was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.

- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Application role (page description)

To open the **Entitlements – Application role** page go to **Responsibilities** > **Auditing** > **Auditing - One Identity Manager application roles** > **Show details** > **Entitlements**.

On the **Entitlements – Application role** page, you can see the entitlements assigned to the application role (see Displaying application role entitlements on page 481).

The following table gives you an overview of the various features and content on the **Entitlements – One Identity Manager application roles** page.

Table 523: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Application role (page description)

To open the **Attestation – Application role** page go to **Responsibilities** > **Auditing** > **Auditing - One Identity Manager application roles** > **Show details** > **Attestation**.

On the **Attestation - Application role** page, you can:

- Display all attestation cases linked to this application role (see Displaying application role pending attestation cases on page 482)
- Display identities that have yet to approve application role attestation cases (see Displaying attestors of application role pending attestation cases on page 484)
- Display details of the objects being attested (see Displaying application role pending attestation cases on page 482)

The following tables give you an overview of the various features and content on the **Attestation - application role** page.

Table 524: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of application role pending attestation cases on page 484).

Table 525: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying application role pending attestation cases on page 482).

Table 526: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Application role (page description)

To open the **Compliance – Application role** page go to **Responsibilities** > **Auditing** > **Auditing - One Identity Manager application roles** > **Show details** > **Compliance**.

- See how the calculated risk index is put together

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

Table 527: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index .

Table 528: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Application role (page description)

To open the **History – Application role** page go to **Responsibilities** > **Auditing** > **Auditing - One Identity Manager application roles** > **Show details** > **History**.

On the **History – Application role** page, you can see all the changes made to the application role (see Application role history on page 485).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect an application role, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you

also see all the steps in between.

- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Application role** page.

Table 529: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying application role history on page 485). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying application role history on page 485).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying application role history on page 485).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of application roles on page 487).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of application roles on page 487).

Table 530: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 531: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.

Column	Description
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Application role (page description)

To open the **Usage – Application Role** page go to **Responsibilities** > **Auditing** > **Auditing - One Identity Manager Application Roles** > **Show details** > **Usage**.

On the **Usage – Application role** page, you can see the roles and organizations that belong to the identities to which this application role is assigned (see Displaying role memberships of application role members on page 488).

The following tables give you an overview of the different functions on the **Usage - Application roles** page.

Table 532: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Device (page description)

To open the **Auditing - Devices** page go to **Responsibilities** > **Auditing** > **Devices**.

On the **Auditing - Devices** page, you can see all the devices (see Displaying devices on page 489).

If you click **Show details** in a device's details pane, a new page opens (see Auditing - Roles and entitlements: device (page description) on page 1195) that contains more information and configuration options for the device.

The following tables give you an overview of the various features and content on the **Auditing - Devices** page.

Table 533: Columns

Column	Description
Display	Shows the device's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and entitlements: device (page description)

To open the **Auditing - Roles and entitlements: Device** page go to **Responsibilities** > **Auditing** > **Devices** > **Show details**.

On the **Auditing - Roles and entitlements: device** page, you can access various information about the selected device.

To do this, click on one of the tiles:

Table 534: Tiles

Tile	Description
Overview	Opens the **Overview - Device** page (see Overview – Device (page description) on page 1196).

Tile	Description
	This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying device overviews on page 489).
Main data	Opens the **Main data - Device** page (see Main data – Device (page description) on page 1196). Here you can see and edit the device's main data (see Displaying device main data on page 490).
Attestation	Opens the **Attestation – Device** page (see Attestations – Device (page description) on page 1199). You select the following actions: • Display all attestation cases linked to this device (see Displaying device attestation cases on page 491) • Display identities that have yet to approve device attestation cases (see Displaying attestors of pending attestation cases for devices on page 492) • Display details of the objects being attested (see Displaying device attestation cases on page 491)

Overview – Device (page description)

To open the **Overview – Device** page go to **Responsibilities** > **Auditing** > **Devices** > **Show details** > **Overview**.

On the **Overview - Device** page, you can see all the information relevant to the device summarized in an overview (see Displaying device overviews on page 489).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Device (page description)

To open the **Main data - Device** page go to **Responsibilities** > **Auditing** > **Devices** > **Show details** > **Main data**.

On the **Main data - Device** page, you can see and edit the device's main data (see Displaying device main data on page 490).

Enter the following main data:

Table 535: Mobile phone main data

Property	Description
Device type	In the menu, select the type of device.
Used by	Click **Change** and select the identity that will use the device.

Property	Description
Device model	Click **Assign**/**Change** and select the device's model.
Manufacturer	Click **Assign**/**Change** and select the manufacturer of the device.
Device ID	Enter a name for the device.
Device status	Click **Assign**/**Change** and select the device's status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
Storage capacity [GB]	Enter the device's storage capacity (in gigabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.
Asset number	Enter the device's asset number.
Company owned	Select the check box if the device belongs to the company.

Table 536: PC main data

Property	Description
Device type	In the menu, select the type of device.
Used by	Click **Change** and select the identity that will use the device.
Device model	Click **Assign**/**Change** and select the device's model.
Manufacturer	Click **Assign**/**Change** and select the manufacturer of the device.
Device ID	Enter a name for the device.
Device status	Click **Assign**/**Change** and select the device's status.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
Storage	Enter the device's storage capacity (in gigabytes).

Property	Description
capacity [GB]	
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
MAC address	Enter the device's MAC address.
PC	Select the check box if this is a simple desktop PC for an identity.
Servers	Select the check box if this is a server.
VM Host	Select the check box if this is a host for a virtual machine.
VM Client	Select the check box if this is a virtual machine.
VM Host	Click **Assign/Change** and select the device you want to install the virtual machine on. The select is available if the **VM Client** check box is set.
MAC address	Enter the device's MAC address.
Asset number	Enter the device's asset number.
Company owned	Select the check box if the device belongs to the company.

Table 537: Tablet main data

Property	Description
Device type	In the menu, select the type of device.
Used by	Click **Change** and select the identity that will use the device.
Device model	Click **Assign/Change** and select the device's model.
Manufacturer	Click **Assign/Change** and select the manufacturer of the device.
Device ID	Enter a name for the device.
Device status	Click **Assign/Change** and select the device's status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
Storage capacity [GB]	Enter the device's storage capacity (in gigabytes).
Operating system	Enter the name of the device's operating system.

Property	Description
Operating system version	Enter the version number of the device's operating system.
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.
Asset number	Enter the number of the asset in the device's bookkeeping.
Company owned	Select the check box if the device belongs to the company.

Attestations – Device (page description)

To open the **Attestation – Device** page go to **Responsibilities** > **Auditing** > **Device** > **Show details** > **Attestation**.

On the **Attestation - Device** page, you can:

- Display all attestation cases linked to this device (see Displaying device attestation cases on page 491)
- Display identities that have yet to approve device attestation cases (see Displaying attestors of pending attestation cases for devices on page 492)
- Display details of the objects being attested (see Displaying device attestation cases on page 491)

The following tables give you an overview of the various features and content on the **Attestations - Device** page.

Table 538: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of pending attestation cases for devices on page 492).

Table 539: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying device attestation cases on page 491).

Table 540: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing – Business roles (page description)

To open the **Auditing - Business Roles** page go to **Responsibilities** > **Auditing** > **Business Roles**.

On the **Auditing - Business Roles** page, you can see all the business roles (see Displaying all business roles on page 493).

If you click **Show details** in a business role's details pane, a new page opens (see Auditing - Roles and entitlements: business role (page description) on page 1201) that contains more information and configuration options for the business role.

The following tables give you an overview of the various features and content on the **Auditing – Business roles** page.

Table 541: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the business roles they manage are shown(see Displaying all business roles on page 493).

Table 542: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - Roles and entitlements: business role** page (see Auditing - Roles and entitlements: business role (page description) on page 1201). Use this button to display more details about the business role.

Table 543: Columns

Column	Description
Display	Shows the business role's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and entitlements: business role (page description)

To open the **Auditing - Roles and entitlements: business role** page go to **Responsibilities** > **Auditing** > **Business Roles** > **Show details**.

On the **Auditing - Roles and entitlements: business role** page, you can access various information about the selected business role.

To do this, click on one of the tiles:

Table 544: Tiles

Tile	Description
Overview	Opens the **Overview – Business role** page (see Overview – Business role (page description) on page 1203). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying business role overviews on page 494).
Main data	Opens the **Main data – Business role** page (see Main data – Business role (page description) on page 1203).

Tile	Description
	Here you see the business role's main data (see Displaying business role main data on page 495).
Memberships	Opens the **Memberships – Business role** page (see Memberships – Business role (page description) on page 1204). Here you can display identities to which the business role is assigned (see Displaying memberships in business roles on page 495).
Entitlements	Opens the **Entitlements – Business role** page (see Entitlements – Business role (page description) on page 1205). Here you can see the entitlements assigned to the business role (see Displaying business role entitlements on page 496).
Attestation	Opens the **Attestation – Business role** page (see Attestation – Business role (page description) on page 1205). You select the following actions: • Display all attestation cases linked to this business role (see Displaying business role attestation cases on page 497) • Display identities that have yet to approve business role attestation cases (see Displaying attestors of business role pending attestation cases on page 498) • Display details of the objects being attested (see Displaying business role attestation cases on page 497)
Compliance	Opens the **Compliance – Business role** page (see Compliance – Business role (page description) on page 1206). Here you see compliance rule violations that were caused by this business role (see Displaying business role rule violations on page 500).
Risk	Opens the **Risk – Business role** page (see Risk – Business role (page description) on page 1207). Here you can see the business role's risk index (see Displaying business role risk indexes on page 500). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – Business role** page (see History – Business role (page description) on page 1208). Here you can see all the changes made to the business role (see Business role history on page 501).
Usage	Opens the **Usage – Business role** page (see Usage – Business role (page description) on page 1210). Here you can see which roles the members of the business role belong

Tile	Description
	to (see Displaying role memberships of business role members on page 504).

Overview – Business role (page description)

To open the **Overview – Business Role** page go to **Responsibilities** > **Auditing** > **Business Roles** > **Show details** > **Overview**.

On the **Overview - Business role** page, you can see all the information relevant to the business role summarized in an overview (see Displaying business role overviews on page 494).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Business role (page description)

To open the **Main data – Business Role** page go to **Responsibilities** > **Auditing** > **Business Roles** > **Show details** > **Main data**.

On the **Main data – Business role** page, you can see the business role's main data (see Displaying business role main data on page 495).

Enter the following main data:

Table 545: Business role main data

Property	Description
Business role	Shows the full, descriptive name of the business role.
Short name	Shows the business role's short name.
Internal name	Shows the company internal name of the business role.
Role class	Shows the business role's role class. To differentiate between different business roles, define company specific role classes. Role classes are used to specify which company resource assignments are possible through roles in a role class.
Parent business role	Shows the parent business role of this business role. If the business role is at the root of a business role hierarchy, the field is empty.
Role type	Shows the business role's role type. Role types are mainly used to regulate approval policy inheritance.
Role approver	Shows the role approver. Members of the selected application role can approve requests for

Property	Description
	members of the business role.
Role approver (IT)	Shows the IT application role approver. Members of the selected application role can approve requests for members of the business role.
Manager	Shows the identity responsible for the business role.
2nd Manager	Shows the identity acting as a deputy to the business role's manager.
identitys do not inherit	Shows whether identities for this business role are temporarily prevented from inheriting.
Description	Shows the business role's description.
Comment	Shows an informative comment about the business role.

Memberships – Business role (page description)

To open the **Memberships – Business Role** page go to **Responsibilities** > **Auditing** > **Business Roles** > **Show details** > **Memberships**.

On the **Memberships - Business Role** page, you can see identities to which the business role is assigned (see Displaying memberships in business roles on page 495).

The following table gives an overview of the different content on the **Memberships – Business role** page.

Table 546: Columns

Column	Description
Identity	Shows you the name of the identity to which the business role is assigned.
Origin	Shows you whether the business role was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Business role (page description)

To open the **Entitlements – Business Role** page go to **Responsibilities** > **Auditing** > **Business Roles** > **Show details** > **Entitlements**.

On the **Entitlements – Business role** page, you can see the entitlements assigned to the business role (see Displaying business role entitlements on page 496).

The following table gives an overview of the content of the **Entitlements – Business role** page.

Table 547: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Business role (page description)

To open the **Attestation – Business Role** page go to **Responsibilities** > **Auditing** > **Business Roles** > **Show details** > **Attestation**.

On the **Attestation - Business role** page, you can:

- Display all attestation cases linked to this business role (see Displaying business role attestation cases on page 497)
- Display identities that have yet to approve business role attestation cases (see Displaying attestors of business role pending attestation cases on page 498)
- Display details of the objects being attested (see Displaying business role attestation cases on page 497)

The following tables give you an overview of the various features and content on the **Attestation - Business role** page.

Table 548: Controls

Control	Description
View approvers for pending	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder

Control	Description
cases	emails to these identities (see Displaying attestors of business role pending attestation cases on page 498).

Table 549: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying business role attestation cases on page 497).

Table 550: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Business role (page description)

Open the **Compliance – Business Role** page by navigating through **Responsibilities** > **Auditing** > **Business Roles** > **Show details** > **Compliance**.

On the **Compliance – Business role** page, you can see compliance rule violations connected with this business role (see Displaying business role rule violations on page 500).

The following table gives an overview of the content of the **Compliance – Business role** page.

Table 551: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Business role (page description)

Open the **Compliance – Business Role** page by navigating through **Responsibilities** > **Auditing** > **Business Roles** > **Show details** > **Compliance**.

On the **Risk – Business role** page, you can:

- Display the business role's calculated risk index (see Displaying business role risk indexes on page 500)
- See how the calculated risk index is put together (see Displaying business role risk indexes on page 500)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – Business role** page.

Table 552: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying business role risk indexes on page 500).

Table 553: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Business role (page description)

To open the **History – Business Role** page go to **Responsibilities** > **Auditing** > **Business Roles** > **Show details** > **History**.

On the **History – Business Role** page you can see all changes made to the business role (see Business role history on page 501).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a business role, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Business role** page.

Table 554: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying business role history on page 501). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying business role history on page 501).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying business role history on page 501).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of business roles on page 503).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of business roles on page 503).

Table 555: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 556: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.

Column	Description
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Business role (page description)

To open the **Usage – Business Role** page go to **Responsibilities** > **Auditing** > **Business Roles** > **Show details** > **Usage**.

On the **Usage – Business role** page, you can see the roles and organizations that belong to the identities to which this business role is assigned (see Displaying role memberships of business role members on page 504).

The following table gives you an overview of the various features on the **Usage - Business roles** page.

Table 557: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Identity details (page description)

To open the **Auditing - Identity Details** page go to **Responsibilities** > **Auditing** > **Identities**.

On the **Auditing - Identity Details** page, you can see all identities (see Displaying all identities on page 505).

If you click an identity in the list, a new page opens (see Auditing – Identity (page description) on page 1211) that contains more information and configuration options for the identity.

The following table gives you an overview of the various features and content on the **Attestation - Identity Details** page.

Table 558: Columns

Column	Description
Display	Shows you the identity's name.
Primary department	Shows the department that the identity is primarily assigned to.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing – Identity (page description)

To open the **Auditing – Identity** page go to **Responsibilities** > **Auditing** > **Identities** > select an identity.

On the **Auditing - Identity** page, you can access various information about the selected identity.

To do this, click on one of the tiles:

Table 559: Tiles

Tile	Description
Overview	Opens the **Overview - Identity** page (see Overview – Identity (page description) on page 1213). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying identity overviews on page 506).
Main data	Opens the **Main data – Identity** page (see Main data – Identity (page description) on page 1213). Here you see the identity's main data (see Displaying identity main data on page 506).

Tile	Description
Requests	Opens the **Requests – Identity** page (see Requests - Identities ((page description)) on page 1215). Here you can see all the products that this identity has requested or were requested for it (see Displaying identity requests on page 507).
Approvals	Opens the **Approvals – Identity** page (see Approvals – Identity (page description) on page 1217). Here you can: • Display all approval processes for product requests that the identity was involved in and their approval decisions (see Displaying identity approvals on page 507). • Display all rule violations that were dealt with by the identity (see Displaying identity approvals on page 507) • Display all approval processes for attestation that the identity was involved in and their approval decisions.Displaying identity approvals on page 507 • Display all policy violations dealt with by the selected identity (see Displaying identity approvals on page 507)
Entitlements	Opens the **Entitlements – Identity** page (see Entitlements – Identity (page description) on page 1221). Here you can see the entitlements assigned to the identity (see Displaying identity entitlements on page 508).
Responsibilities	Opens the **Responsibilities – Identity** page (see Responsibilities - Identity (page description) on page 1222). Here you can see all the objects for which the identity is responsible (see Displaying identity responsibilities on page 509).
Attestation	Opens the **Attestation – Identity** page (see Attestations – Identity (page description) on page 1222). You select the following actions: • Display all attestation cases linked to this identity (see Displaying attestation cases of identities on page 510) • Display identities that have yet to approve identity attestation cases (see Displaying attestors of identity pending attestation cases on page 511) • Display details of the objects being attested (see Displaying attestation cases of identities on page 510)
Rule violations	Opens the **Rule Violations – Identity** page (see Rule violations – Identity (page description) on page 1224).

Tile	Description
	Here you can see rule violations that were caused by this identity (see Displaying identities' rule violations on page 513).
Compliance	Opens the **Compliance – Identity** page (see Compliance – Identity (page description) on page 1225). Here you can see compliance rule violations that were caused by this identity (see Displaying identities' rule violations on page 513).
Risk	Opens the **Risk – Identity** page (see Risk – Identity (page description) on page 1225). Here you can see the identity's risk index (see Displaying identity risk indexes on page 514). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – Identity** page (see History – Identity (page description) on page 1226). Here you can see all the changes made to the identity (see Identity history on page 514).

Overview – Identity (page description)

To open the **Overview - Identity** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **Overview**.

On the **Overview - Identity** page, you can see all the information relevant to the identity summarized in an overview (see Displaying identity overviews on page 506).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Identity (page description)

To open the **Main data – Identity** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **Main data**.

On the **Main data - Identity** page, you can see and edit the identity's main data (see Displaying identity main data on page 506).

Enter the following main data:

Table 560: Identities main data

Property	Description
Personal data	
Last name	Shows the identity's last name.

Property	Description
First name	Shows the identity's first name.
Date of birth	Shows the identity's date of birth.
Personnel number	Shows the identity's personnel number.
Gender	Shows the identity's gender
Central user account	Shows the name of the identity's central user account.
Default email address	Shows the identity's default email address.
Organizational information	
Primary cost center	Shows the cost center that the identity is primarily assigned to.
Primary department	Shows the department that the identity is primarily assigned to.
External	Identifies the identity as external.
Employee type	Identifies the identity as a company employee or a trainee (for example).
Entry date	Shows the date the identity started at the company.
End date	Shows the date that the identity leaves the company.
Manager	Shows the identity's manager.
Temporarily disable until	Shows whether the identity is temporarily deactivated (for example, due to leave, sickness or pregnancy).
Locational information	
Primary location	Shows the identity's primary location.
Building	Shows the building where the identity works.
Floor	Shows the floor the identity works on.
Room	Shows the room the identity works in.
Street	Shows the street where the identity works.
Zip code	Shows the zip code of the identity's work location.
City	Shows the city where the identity works.

Requests - Identities ((page description))

To open the **Requests – Identity** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **Requests**.

On the **Requests - Identity** page you can see all the products an identity has requested or that have been requested for them (see Displaying identity requests on page 507).

The following tables give you an overview of the various features and content on the **Requests – Identity** page.

Table 561: Controls

Control	Description
Advanced search	The advanced search allows you to control which product requests are displayed: • **Requests submitted by the selected identity for itself**: Select this check box to display product requests placed by the selected identity for themselves. • **Requests submitted by the selected identity for others**: Select this check box to display product requests placed by the selected identity for other identities. • **Requests submitted by others for the selected identity**: Select this check box to display product requests placed by other identities for the selected identity. • **Submitted requests in the selected identity's organization**: Select this check box to display product requests placed in the selected identity's scope of responsibility. • **Filter by request number**: Enter the request number of the request you want to display. • **pending**: Select this check box to display product requests that are not yet approved (status: **Request**). • **Approved**: Select this check box to display product requests that have been granted approval (status: **Assigned**). • **Canceled or denied or unsubscribed**: Select this check box to display product requests that have been canceled, denied, or unsubscribed. Click **Search** to apply the filter criteria to the request history. Click **Reset** to reset the filter criteria to the default search.

Table 562: Columns

Column	Description
Product	Shows the name of the product that was requested.

Column	Description
State	Shows the current status of the product. The following status' are possible: • **Assigned**: The product request was successful and the product was successfully assigned. • **Request**: The product request is still awaiting an approval decision (it is still in the request workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The product request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The product request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Renewal**: The product has been renewed (see Renewing products with limit validity periods on page 130). • **Unsubscription**: The product is being unsubscribed (see Unsubscribing products on page 131). • **Denied**: The request for this product was denied. The reason for denying may be a policy or rule violation or the manager not verifying the request if it is only temporary. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. . • **Canceled**: The product request was canceled or the system could not carry out the request (for example, because an identity for verifying it was not given or the validity period expired). In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed**: The product was unsubscribed (see Unsubscribing products on page 131). In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested. TIP: If you only want to display products that were requested within a certain time period, click **Filtering: Request date** next to the column header and select the appropriate options.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows you the request number of the total request with which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Approvals – Identity (page description)

To open the **Approvals – Identity** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **Approvals**.

On the **Approvals – identity** page you can:

- Display all approval processes for product requests that the identity was involved in and their approval decisions (see Displaying identity approvals on page 507).
- Display all rule violations that were dealt with by the identity (see Displaying identity approvals on page 507)
- Display all approval processes for attestation that the identity was involved in and their approval decisions.Displaying identity approvals on page 507
- Display all policy violations dealt with by the selected identity (see Displaying identity approvals on page 507)

The information is divided into the following tabs:

- **Approvals**

  NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

  - **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
  - **Workflow**: Displays the life cycle chronologically as from the time of request.
  - **Compliance**: Displays possible rule violations for this request.
- **Exception approvals**

  TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

  - **Rule violation**: Shows you general information about the rule violation.
  - **Rule**: Shows you general information about the rule that was violated.
- **Attestations**

  NOTE: On the following tabs, you can show other useful information about each instance in the details pane. To do this, click the appropriate instance in the list.

- **Information**: Displays general information about the attestations case.
- **Workflow**: Shows the chronological lifecycle of the attestation case.
- **Attestation policy**: Shows further information about the attestation policy used.
- **History**: Shows the object's attestation history.

- **Policy violations**

  TIP: On the following tabs in the details pane, you can view other useful information about each rule violation. To do this, click the corresponding entry in the list.

  - **Policy violation**: Shows you general information about the policy violation.
  - **Object**: Shows you general information about object that was violated the policy.
  - **Policy**: Shows you general information about policy that was violated.

The following tables give you an overview of the various features and content on the **Approvals – Identity** page.

Table 563: Controls

Control	Description
Approvals tab	
Advanced search	The advanced search allows you to control which product requests are displayed: • **Filter by request number**: Enter the request number of the request you want to display. • **pending**: Select this check box to display product requests that are not yet approved (status: **Request**). • **Approved**: Select this check box to display product requests that have been granted approval (status: **Assigned**). • **Canceled or denied or unsubscribed**: Select this check box to display product requests that have been canceled, denied, or unsubscribed. Click **Search** to apply the filter criteria to the request history. Click **Reset** to reset the filter criteria to the default search.
Attestation tab	
Attestation state	The check boxes allow you to control which approvals are displayed: • **Approved**: Select this check box to display attestation cases that have been granted approval. • **Pending**: Select this check box to display attestation cases that you have made an approval decision about but have not yet been approved.

Control	Description
	• **Not approved**: Select this check box to display attestation cases that have been denied.
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and send them reminder mails (see Displaying attestors of identity pending attestation cases on page 511).

Table 564: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to view all identities that can make approval decisions about the attestation case (see Displaying attestors of identity pending attestation cases on page 511). Then you can send them reminder mails.
Viewing details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying attestation cases of identities on page 510).

Table 565: Columns

Column	Description
Approvals tab	
Product	Shows the name of the product that was requested.
State	Shows the current status of the product. The following status' are possible: • **Assigned**: The product request was successful and the product was successfully assigned. • **Request**: The product request is still awaiting an approval decision (it is still in the request workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The product request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The product request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Renewal**: The product has been renewed (see Renewing products with limit validity periods on page 130). • **Unsubscription**: The product is being unsubscribed (see Unsubscribing products on page 131).

Column	Description
	• **Denied**: The request for this product was denied. The reason for denying may be a policy or rule violation or the manager not verifying the request if it is only temporary. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. . • **Canceled**: The product request was canceled or the system could not carry out the request (for example, because an identity for verifying it was not given or the validity period expired). In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed**: The product was unsubscribed (see Unsubscribing products on page 131). In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested. TIP: If you only want to display products that were requested within a certain time period, click **Filtering: Request date** next to the column header and select the appropriate options.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows you the request number of the total request with which the product was requested.
Exception approvals tab	
Rule violation	Shows you the name of the violated rule.
Approval state	Shows you whether the exception was approved or denied. The following status' are possible: • **Exception granted**: The exception was approved. In the details pane, on the **Rule violation** tab, you can see why the exception was granted approval. • **Exception denied**: The exception was denied. In the details pane, on the **Rule violation** tab, you can see why the exception was denied approval.
Risk index (reduced)	Shows you the risk index reduced by the mitigating control.
Attestation tab	
Display name	Shows the name of the object included in the attestation case.
Attestation	Shows the name of the attestation policy in use.

Column	Description
policy	
State	Shows the current status of the attestation case. The following status' are possible: • **Approved**: The attestation case was approved. • **Pending**: The attestation case is not closed yet and must still be approved. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.
Policy violations tab	
Violating object	Show which object violated the policy.
Policy	Shows the name of the violated policy.
State	Shows you whether the exception was approved or denied. The following status' are possible: • **Exception granted**: The exception was approved. In the details pane, on the **Policy violation** tab, you can see why the exception was granted approval. • **Exception denied**: The exception was denied. In the details pane, on the **Policy violation** tab, you can see why the exception was denied approval.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Identity (page description)

To open the **Entitlements – Identity** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **Entitlements**.

On the **Entitlements – Identity** page, you can see the entitlements assigned to the cost center (see Displaying identity entitlements on page 508).

The following table gives you an overview of the various features and content on the **Entitlements – Identity** page.

Table 566: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Object type	Shows you the entitlement type (for example, if it is a system role)
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Responsibilities - Identity (page description)

To open the **Responsibilities – <identity>** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **Responsibilities**.

On the **Responsibilities - Identity** page, you can see all objects for which the identity is responsible (see Displaying identity responsibilities on page 509).

The following table gives you an overview of the various features on the **Responsibilities – <identity>** page.

Table 567: Controls

Control	Description
Object type	Use this drop-down to select which of objects managed by the identity you want to display (for example, departments).

Table 568: Controls in the details pane of an object

Control	Description
Viewing details	Use this button to display the object's details (see Displaying identity responsibilities on page 509).

Table 569: Columns

Column	Description
Display	Shows you the name of the object for which the identity is responsible.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – Identity (page description)

To open the **Attestation – Identity** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **Attestation**.

On the **Attestation - Identity** page, you can:

- Display all attestation cases linked to this identity (see Displaying attestation cases of identities on page 510)
- Display identities that have yet to approve identity attestation cases (see Displaying attestors of identity pending attestation cases on page 511)
- Display details of the objects being attested (see Displaying attestation cases of identities on page 510)

The following table gives an overview of the various content of the **Attestation - Identity** page.

Table 570: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of identity pending attestation cases on page 511).

Table 571: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of identities on page 510).

Table 572: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.

Column	Description
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Rule violations – Identity (page description)

To open the **Rule Violations – <identity>** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **Rule Violations**.

On the **Rule Violations – <identity>** page, you can see compliance rule violations connected with this identity (see Displaying identities' rule violations on page 513).

The following table gives an overview of the various content of the **Rule Violations - <identity>** page.

Table 573: Columns

Column	Description
Employee	Shows you the name of the identity that violated the rule.
Rule violation	Shows you the name of the violated rule.
Approval state	Shows you whether the exception was approved or denied. The following status' are possible: • **Exception granted**: The exception was approved. In the details pane, on the **Rule violation** tab, you can see why the exception was granted approval. • **Exception denied**: The exception was denied. In the details pane, on the **Rule violation** tab, you can see why the exception was denied approval.
Risk index (reduced)	Shows you the risk index reduced by the mitigating control.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Rule violation**: Shows you general information about the rule violation.
- **Rule**: Shows you general information about the rule that was violated.

Compliance – Identity (page description)

Open the **Compliance – Identity** page by navigating through **Responsibilities** > **Auditing** > **Identities** > select identity > **Compliance**.

On the **Compliance – Identity** page, you can see compliance rule violations connected with this identity (see Displaying identities' rule violations on page 513).

The following table gives an overview of the content of the **Compliance – Identity** page.

Table 574: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Identity (page description)

To open the **Compliance – Identity** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **Compliance**.

On the **Risk – Identity** page, you can:

- Display the identity's calculated risk index (see Displaying identity risk indexes on page 514)
- See how the calculated risk index is put together (see Displaying identity risk indexes on page 514)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the various features and content on the **Risk – Identity** page.

Table 575: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying identity risk indexes on page 514).

Table 576: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Identity (page description)

To open the **History – Identity** page go to **Responsibilities** > **Auditing** > **Identities** > select identity > **History**.

On the **History – Identity** page, you can see all the changes made to the identity (see Identity history on page 514).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows you all events concerning the identity, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the various features and content on the **History – Identity Details** page.

Table 577: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying identity history on page 515). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying identity history on page 515).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying identity history on page 515).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of identities on page 516).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of identities on page 516).

Table 578: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 579: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.

Column	Description
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing – Cost center (page description)

Open the **Auditing - Cost centers** page by navigating through **Responsibilities** > **Auditing** > **Cost centers**.

On the **Auditing - Cost centers** page, you can see all the cost centers (see Displaying all cost centers on page 518).

If you click **Show details** in a cost center's details pane, a new page opens (see Auditing - Roles and entitlements: cost center (page description) on page 1229) that contains more information and configuration options for the cost center.

The following tables give you an overview of the various features and content on the **Auditing – Cost centers** page.

Table 580: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the cost centers they manage are shown (see Displaying all cost centers on page 518).

Table 581: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - Roles and entitlements: cost center** page (see Auditing - Roles and entitlements: cost center (page description) on page 1229). Use this button to display more details about the cost center.

Table 582: Columns

Column	Description
Display	Shows the cost center's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and entitlements: cost center (page description)

To open the **Auditing - Roles and entitlements: cost center** page go to **Responsibilities** > **Auditing** > **Cost centers** > **Show details**.

On the **Auditing - Roles and entitlements: cost center** page, you can access various information about the selected cost center.

To do this, click on one of the tiles:

Table 583: Tiles

Tile	Description
Overview	Opens the **Overview – Cost center** page (see Overview – Cost center (page description) on page 1231). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying cost center overviews on page 518).
Main data	Opens the **Main data – Cost center** page (see Main data – Cost center (page description) on page 1231). Here you see the cost center's main data (see Displaying cost center

Tile	Description
	main data on page 519).
Memberships	Opens the **Memberships – Cost center** page (see Memberships – Cost center (page description) on page 1232). Here you can see identities assigned to the cost center (see Displaying memberships in cost centers on page 519).
Entitlements	Opens the **Entitlements – Cost center** page (see Entitlements – Cost center (page description) on page 1232). Here you can display the entitlements assigned to the cost center (see Displaying cost center entitlements on page 520).
Attestation	Opens the **Attestation – Cost center** page (see Attestation – Cost center (page description) on page 1233). You select the following actions: • Display all attestation cases linked to this cost center (see Displaying cost center attestation cases on page 521) • Display identities that have yet to approve cost center attestation cases (see Displaying attestors of cost center pending attestation cases on page 522) • Display details of the objects being attested (see Displaying cost center attestation cases on page 521)
Compliance	Opens the **Compliance – Cost center** page (see Compliance – Cost center (page description) on page 1234). Here you can see compliance rule violations that were caused by this cost center (see Displaying cost center rule violations on page 524).
Risk	Opens the **Risk – Cost center** page (see Risk – Cost center (page description) on page 1235). Here you can see the cost center's risk index (see Displaying cost center risk indexes on page 524). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – Cost center** page (see History – Cost center (page description) on page 1236). Here you can see all the changes made to the cost center (see Cost center history on page 525).
Usage	Opens the **Usage – Cost center** page (see Usage – Cost center (page description) on page 1238). Here you can see which roles the members of the cost center belong to (see Displaying role memberships of cost center members on page 528).

Overview – Cost center (page description)

To open the **Overview – Cost center** page go to **Responsibilities** > **Auditing** > **Cost centers** > **Show details** > **Overview**.

On the **Overview – Cost center** page, you can see all the information relevant to the cost center summarized in an overview (see Displaying cost center overviews on page 518.)

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Cost center (page description)

Open the **Main data – Cost center** page by navigating through **Responsibilities** > **Auditing** > **Cost centers** > **Show details** > **Main data**.

On the **Main data – Cost center** page, you can see the cost center's main data (see Displaying cost center main data on page 519).

Enter the following main data:

Table 584: Cost center main data

Property	Description
Cost center	Shows the full, descriptive name of the cost center.
Short name	Shows the cost center's short name.
Location	Shows the location that the cost center is primarily assigned to.
Parent cost center	Shows the parent cost center of this cost center. If the cost center is at the root of a cost center hierarchy, the field is empty.
Attestors	Shows the attestor application role. Members of this application role can approve attestation cases for the cost center.
Department	Shows the department assigned to the cost center.
Role approver	Shows the role approver. Members of the selected application role can approve requests for members of the cost center.
Role approver (IT)	Shows the IT application role approver. Members of the selected application role can approve requests for members of the cost center.
Manager	Shows the identity responsible for the cost center.
2nd Manager	Shows the identity acting as a deputy to the cost center's manager.
Description	Shows the cost center's description.

Memberships – Cost center (page description)

To open the **Memberships – Cost center** page go to **Responsibilities** > **Auditing** > **Cost centers** > **Show details** > **Memberships**.

On the **Memberships - Cost Center** page, you can see identities assigned to the cost center (see Displaying memberships in cost centers on page 519).

The following table gives an overview of the different content on the **Memberships – Cost center** page.

Table 585: Columns

Column	Description
Identity	Shows you the name of the identity assigned to the cost center.
Origin	Shows you whether the cost center was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Cost center (page description)

To open the **Entitlements – Cost center** page go to **Responsibilities** > **Auditing** > **Cost centers** > **Show details** > **Entitlements**.

On the **Entitlements – Cost center** page, you can see the entitlements assigned to the cost center (see Displaying cost center entitlements on page 520).

The following table gives you an overview of the various features and content on the **Entitlements – application roles** page.

Table 586: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Cost center (page description)

To open the **Attestation – Cost center** page go to **Responsibilities** > **Auditing** > **Cost centers** > **Show details** > **Attestation**.

On the **Attestation - Cost center** page, you can:

- Display all attestation cases linked to this cost center (see Displaying cost center attestation cases on page 521)
- Display identities that have yet to approve cost center attestation cases (see Displaying attestors of cost center pending attestation cases on page 522)
- Display details of the objects being attested (see Displaying cost center attestation cases on page 521)

The following tables give you an overview of the various features and content on the **Attestation - Cost center** page.

Table 587: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of cost center pending attestation cases on page 522).

Table 588: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying cost center attestation cases on page 521).

Table 589: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Cost center (page description)

Open the **Compliance – Cost center** page by navigating through **Responsibilities** > **Auditing** > **Cost centers** > **Show details** > **Compliance**.

On the **Compliance – Cost center** page, you can see compliance rule violations connected with this cost center (see Displaying cost center rule violations on page 524).

The following table gives an overview of the content of the **Compliance – System role** page.

Table 590: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation

Column	Description
	poses.
Risk index	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Cost center (page description)

To open the **Compliance – Cost center** page go to **Responsibilities** > **Auditing** > **Cost centers** > **Show details** > **Compliance**.

On the **Risk – Cost center** page, you can:

- Display the cost center's calculated risk index (see Displaying cost center risk indexes on page 524)
- See how the calculated risk index is put together (see Displaying cost center risk indexes on page 524)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – Cost center** page.

Table 591: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying cost center risk indexes on page 524).

Table 592: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.

Column	Description
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Cost center (page description)

To open the **History – Cost center** page go to **Responsibilities** > **Auditing** > **Cost centers** > **Show details** > **History**.

On the **History – Cost center** page, you can see all the changes made to the cost center (see Cost center history on page 525).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a cost center, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.
- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Cost center** page.

Table 593: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying cost center history on page 526). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.

Control	Description
Switch to table view	Use this button to display the changes in table form (see Displaying cost center history on page 526).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying cost center history on page 526).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of cost centers on page 527).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of cost centers on page 527).

Table 594: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 595: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.

Column	Description
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Cost center (page description)

To open the **Usage – Cost center** page go to **Responsibilities** > **Auditing** > **Cost centers** > **Show details** > **Usage**.

On the **Usage – Cost center** page, you can see the roles and organizations that belong to the identities to which this cost center is assigned (see Displaying role memberships of cost center members on page 528).

The following table gives you an overview of the various features on the **Usage - Cost centers** page.

Table 596: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Multi-request resources (page description)

Open the **Auditing - Multi-request resources** page by navigating through **Responsibilities** > **Auditing** > **Multi-request resources**.

On the **Auditing - Multi-request resources** page, you can see all the multi-request resources (see Displaying multi-request resources on page 529).

If you click **Show details** in a multi-request resource's details pane, a new page opens (see Auditing - Roles and entitlements: multi-request resource (page description) on page 1239) that contains more information and configuration options for the multi-request resource.

The following tables give you an overview of the various features and content on the **Auditing – Multi-request resources** page.

Table 597: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the multi-request resources they manage are shown (see Displaying multi-request resources on page 529).

Table 598: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: multi-request resource** page (see Auditing - Roles and entitlements: multi-request resource (page description) on page 1239). Use this button to display more details about the multi-request resource.

Table 599: Columns

Column	Description
Display	Shows the multi-request resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and entitlements: multi-request resource (page description)

To open the **Auditing - Roles and entitlements: multi-request resource** page go to **Responsibilities** > **Auditing** > **Multi-request resources** > **Show details**.

On the **Auditing - Roles and entitlements: multi-request resource** page, you can access various information about the selected multi-request resource.

To do this, click on one of the tiles:

Table 600: Tiles

Tile	Description
Overview	Opens the **Overview – Multi-request resource** page (see Overview – Multi-request resource (page description) on page 1240). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying multi-request resource overviews on page 530).
Main data	Opens the **Main data – Multi-request resource** page (see Main data – Multi-request resource (page description) on page 1240). Here you see the multi-request resource's main data (see Displaying multi-request resource main data on page 530).
Attestation	Opens the **Attestation – Multi-request resource** page (see Attestation – Multi-request resource (page description) on page 1241). You select the following actions: • Display all attestation cases linked to this multi-request resource (see Displaying multi-request resource attestation cases on page 532) • Display identities that have yet to approve multi-request resource attestation cases (see Displaying attestors of multi-request resource pending attestation cases on page 533) • Display details of the objects being attested (see Displaying multi-request resource attestation cases on page 532)

Overview – Multi-request resource (page description)

To open the **Overview – Multi-request resource** page go to **Responsibilities** > **Auditing** > **Multi-request resources** > **Show details** > **Overview**.

On the **Overview – Multi-request resource** page, you can see all the information relevant to the multi-request resource summarized in an overview (see Displaying multi-request resource overviews on page 530).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Multi-request resource (page description)

Open the **Main data – Multi-request resource** page by navigating through **Responsibilities** > **Auditing** > **Multi-request resources** > **Show details** > **Main data**.

On the **Main data - Multi-request resource** page, you can see the multi-request resource's main data (see Displaying multi-request resource main data on page 530).

Enter the following main data:

Table 601: multi-request resource main data

Property	Description
Multi-request resource	Shows the full, descriptive name of the multi-request resource.
Resource type	Shows the type of resource. Use resource types to group multi-request resources.
Description	Shows the multi-request resource's description.
IT Shop	Shows whether the multi-request resource can be requested in the IT Shop. If set, the multi-request resource can be requested by identities using the Web Portal and granted through a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows whether the multi-request resource can only be requested through the IT Shop. If set, the multi-request resource can be requested by identities using the Web Portal and granted through a defined approval process. It is not possible to assign a multi-request resource directly to roles outside of the IT Shop (for example in the Manager).
Service item	Shows assigned service items.
Risk index	Shows the configured risk index. This value specifies the risk of assigning this multi-request resource to an identity.

Attestation – Multi-request resource (page description)

To open the **Attestation – Multi-request resource** page go to **Responsibilities** > **Auditing** > **Multi-request resources** > **Show details** > **Attestation**.

On the **Attestation - Multi-request resource** page, you can:

- Display all attestation cases linked to this multi-request resource (see Displaying multi-request resource attestation cases on page 532)
- Display identities that have yet to approve multi-request resource attestation cases (see Displaying attestors of multi-request resource pending attestation cases on page 533)
- Display details of the objects being attested (see Displaying multi-request resource attestation cases on page 532)

The following tables give you an overview of the various features and content on the **Attestation - Multi-request resource** page.

Table 602: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of multi-request resource pending attestation cases on page 533).

Table 603: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying multi-request resource attestation cases on page 532).

Table 604: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing – Multi requestable/unsubscribable resources (page description)

To open the **Auditing - Multi requestable/unsubscribable resources** page go to **Responsibilities** > **Auditing** > **Multi requestable/unsubscribable resources**.

On the **Auditing - Multiple requestable/unsubscribable resources** page, you can see all the multiple requestable/unsubscribable resources (see Displaying all multi requestable/unsubscribable resources on page 534).

If you click **Show details** in a multiple requestable/unsubscribable resource's details pane, a new page opens (see Auditing - Roles and entitlements: multi requestable/unsubscribable resource (page description) on page 1244) that contains more information and configuration options for the multiple requestable/unsubscribable resource.

The following tables give you an overview of the various features and content on the **Auditing – Multi requestable/unsubscribable resources** page.

Table 605: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the multi requestable/unsubscribable resources they manage are shown (see Displaying all multi requestable/unsubscribable resources on page 534).

Table 606: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - Roles and entitlements: multiple requestable/unsubscribable resource** page (see Auditing - Roles and entitlements: multi requestable/unsubscribable resource (page description) on page 1244). Use this button to display more details about the multiple requestable/unsubscribable.

Table 607: Columns

Column	Description
Display	Shows the multi requestable/unsubscribable resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and entitlements: multi requestable/unsubscribable resource (page description)

To open the **Auditing - Roles and entitlements: multi requestable/unsubscribable resources** page go to **Responsibilities** > **Auditing** > **Multi requestable/unsubscribable resources** > **Show details**.

On the **Auditing - Roles and entitlements: multi requestable/unsubscribable resource** page, you can access various information about the selected multi requestable/unsubscribable resource.

To do this, click on one of the tiles:

Table 608: Tiles

Tile	Description
Overview	Opens the **Overview – Multi requestable/unsubscribable resource** page (see Overview – Multi requestable/unsubscribable resource (page description) on page 1245). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying multi requestable/unsubscribable resource overviews on page 535).
Main data	Opens the **Main data - Multi requestable/unsubscribable resource** page (see Main data – Multi requestable/unsubscribable resource (page description) on page 1245). Here you see the multi-requestable/unsubscribable resource's main data (see Auditing multi requestable/unsubscribable resources on page 534).
Memberships	Opens the **Memberships – Multi requestable/unsubscribable resource** page (see Memberships – Multi requestable/unsubscribable resource (page description) on page 1246).
Attestation	Opens the **Attestation – Multi-requestable/unsubscribable resource** page (see Attestation – Multi requestable/unsubscribable resource (page description) on page 1247). You select the following actions: • Display all attestation cases linked to this multi requestable/unsubscribable resource (see Displaying multi requestable/unsubscribable resource attestation cases on page 537) • Display details of the objects being attested (see Displaying multi requestable/unsubscribable resource attestation cases on page 537)

Overview – Multi requestable/unsubscribable resource (page description)

To open the **Overview – Multi requestable/unsubscribable resource** page go to **Responsibilities** > **Auditing** > **Multi requestable/unsubscribable resources** > **Show details** > **Overview**.

On the **Overview – Multi requestable/unsubscribable resource** page, you can see all the information relevant to the multi requestable/unsubscribable resource summarized in an overview (see Displaying multi requestable/unsubscribable resource overviews on page 535).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Multi requestable/unsubscribable resource (page description)

To open the **Main data – Multi requestable/unsubscribable resource** page go to **Responsibilities** > **Auditing** > **Multi requestable/unsubscribable resources** > **Show details** > **Main data**.

On the **Main data - Multi requestable/unsubscribable resource** page, you can see the multi requestable/unsubscribable resource's main data (see Displaying multi requestable/unsubscribable resource main data on page 535).

Enter the following main data:

Table 609: multi requestable/unsubscribable resource main data

Property	Description
Multi requestable/unsubscribable resource	Shows the full, descriptive name of the multi requestable/unsubscribable resource.
Resource type	Shows the type of resource. Use resource types to group multi requestable/un-subscribable resources.
Description	Shows the multi requestable/unsubscribable resource's description.
IT Shop	Shows whether the multi requestable/unsubscribable resource can be requested in the IT Shop. If set, the multi requestable/unsubscribable resource can be requested by identities using the Web Portal and granted through a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows whether the multi requestable/unsubscribable

Property	Description
	resource can only be requested through the IT Shop. If set, the multi requestable/unsubscribable resource can be requested by identities using the Web Portal and granted through a defined approval process. It is not possible to assign a multi requestable/unsubscribable resource directly to roles outside of the IT Shop (for example in the Manager).
Service item	Shows assigned service items.
Risk index	Shows the configured risk index. This value specifies the risk of assigning this multi requestable/unsubscribable resource to an identity.

Memberships – Multi requestable/unsubscribable resource (page description)

To open the **Memberships – Multi requestable/unsubscribable resource** page go to **Responsibilities** > **Auditing** > **Multi requestable/unsubscribable resources** > **Show details** > **Memberships**.

On the **Memberships – Multi-requestable/unsubscribable resource** page, you can see identities to which multi-requestable/unsubscribable resource is assigned (see Displaying memberships in multi requestable/unsubscribable resources on page 536).

The following table gives an overview of the different content on the **Memberships – Multi requestable/unsubscribable resource** page.

Table 610: Columns

Column	Description
Identity	Shows you the name of the identity to which the multi requestable/unsubscribable resource is assigned.
Origin	Shows you whether the multi requestable/unsubscribable resource was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Multi requestable/unsubscribable resource (page description)

To open the **Attestation – Multi requestable/unsubscribable resource** page go to **Responsibilities** > **Auditing** > **Multi requestable/unsubscribable resources** > **Show details** > **Attestation**.

On the **Attestation - Multi requestable/unsubscribable resource** page, you can:

- Display all attestation cases linked to this multi requestable/unsubscribable resource (see Displaying multi requestable/unsubscribable resource attestation cases on page 537)
- Display details of the objects being attested (see Displaying multi requestable/unsubscribable resource attestation cases on page 537)

The following tables give you an overview of the various features and content on the **Attestation - Multi requestable/unsubscribable resource** page.

Table 611: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of multi requestable/unsubscribable resource pending attestation cases on page 539).

Table 612: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying multi requestable/unsubscribable resource attestation cases on page 537).

Table 613: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.

Column	Description
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Resources (page description)

Open the **Auditing - Resources** page by navigating through **Responsibilities** > **Auditing** > **Resources**.

On the **Auditing - Resources** page, you can see all the resources (see Displaying all resources on page 540).

If you click **Show details** in a resource's details pane, a new page opens (see Auditing - Roles and permissions: resource (page description) on page 1249) that contains more information and configuration options for the resource.

The following tables give you an overview of the various features and content on the **Auditing – resources** page.

Table 614: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the resources they manage are shown (see Displaying all resources on page 540).

Table 615: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: resource** page (see Auditing - Roles and permissions: resource (page description) on page 1249). Use this button to display more details about the resource.

Table 616: Columns

Column	Description
Display	Shows the resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: resource (page description)

To open the **Auditing - Roles and entitlements: resource** page go to **Responsibilities** > **Auditing** > **Resources** > **Show details**.

On the **Auditing - Roles and entitlements: resource** page, you can access various information about the selected resource.

To do this, click on one of the tiles:

Table 617: Tiles

Tile	Description
Overview	Opens the **Overview – Resource** page (see Overview – Resource (page description) on page 1250). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying resource overviews on page 541).
Main data	Opens the **Main data – Resource** page (see Main data – Resource (page description) on page 1250). Here you can see the resource's main data (see Displaying resource main data on page 541).
Memberships	Opens the **Memberships – Resource** page (see Memberships – Resource (page description) on page 1251). Here you can see identities to which the resource is assigned (see Displaying memberships in resources on page 542).

Tile	Description
Attestation	Opens the **Attestation – Resource** page (see Attestation - Resource (page description) on page 1252). You select the following actions: • Display all attestation cases linked to this resource (see Displaying resource attestation cases on page 543) • Display identities that have yet to approve resource attestation cases (see Displaying attestors of resource pending attestation cases on page 544) • Display details of the objects being attested (see Displaying resource attestation cases on page 543)
Usage	Opens the **Usage – Resource** page (see Usage – Resource (page description) on page 1253). Here you can see which roles the members of the resource belong to (see Displaying role memberships resource members on page 545).

Overview – Resource (page description)

To open the **Overview – Resource** page go to **Responsibilities** > **Auditing** > **Departments** > **Show details** > **Overview**.

On the **Overview – Resource** page, you can see all the information relevant to the resource summarized in an overview (see Displaying resource overviews on page 541).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Resource (page description)

To open the **Main data – Resource** page go to **Responsibilities** > **Auditing** > **Resources** > **Show details** > **Main data**.

On the **Main data – Resource** page, you can see the resource's main data (see Displaying resource main data on page 541).

Enter the following main data:

Table 618: Resource main data

Property	Description
Resource	Shows the full, descriptive name of the resource.
Resource type	Shows the type of resource. Use resource types to group resources.
Description	Shows the resource's description.

Property	Description
IT Shop	Shows whether the resource can be requested in the IT Shop. If set, the resource can be requested by identities using the Web Portal and granted through a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows whether the resource can only be requested through the IT Shop. If set, the resource can be requested by identities using the Web Portal and granted through a defined approval process. It is not possible to assign the resource directly to roles outside the IT Shop (for example, in the Manager).
Service item	Shows assigned service items.
Risk index	Shows the configured risk index. This value specifies the risk of assigning this resource to an identity.

Memberships – Resource (page description)

To open the **Memberships – Resource** page go to **Responsibilities** > **Auditing** > **Resources** > **Show details** > **Memberships**.

On the **Memberships - Resource** page, you can see identities to which the resource is assigned (see Displaying memberships in resources on page 542).

The following table gives an overview of the different content on the **Memberships – Resource** page.

Table 619: Columns

Column	Description
Identity	Shows you the name of the identity to which the resource is assigned.
Origin	Shows you whether the resource was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation - Resource (page description)

To open the **Attestation – Resources** page go to **Responsibilities** > **Auditing** > **Resources** > **Show details** > **Attestation**.

On the **Attestation - resource** page, you can:

- Display all attestation cases linked to this resource (see Displaying resource attestation cases on page 543)
- Display identities that have yet to approve resource attestation cases (see Displaying attestors of resource pending attestation cases on page 544)
- Display details of the objects being attested (see Displaying resource attestation cases on page 543)

The following tables give you an overview of the various features and content on the **Attestation - Resource** page.

Table 620: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of resource pending attestation cases on page 544).

Table 621: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying resource attestation cases on page 543).

Table 622: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved.

Column	Description
	• **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Resource (page description)

To open the **Usage – Resources** page go to **Responsibilities** > **Auditing** > **Resources** > **Show details** > **Usage**.

The following tables give you an overview of the different functions on the **Usage - Resources** page.

Table 623: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Software (page description)

Open the **Auditing - Software** page by navigating through **Responsibilities** > **Auditing** > **Software**.

On the **Auditing - Software** page, you can see all the software applications (see Displaying all software applications on page 546).

If you click **Show details** in a software application's details pane, a new page opens (see Auditing - Roles and permissions: Software (page description) on page 1254) that contains more information and configuration options for the software application.

The following tables give you an overview of the various features and content on the **Auditing – Software** page.

Table 624: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the software they manage is shown (see Displaying all software applications on page 546).

Table 625: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: software** page (see Auditing - Roles and permissions: Software (page description) on page 1254). Use this button to display more details about the software application.

Table 626: Columns

Column	Description
Display	Shows the software application's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: Software (page description)

To open the **Auditing - Roles and entitlements: Software** page go to **Responsibilities** > **Auditing** > **Software** > **Show details**.

On the **Auditing - Roles and entitlements: software** page, you can access various information about the selected software application.

To do this, click on one of the tiles:

Table 627: Tiles

Tile	Description
Overview	Opens the **Overview – Software** page (seeOverview - Software (page description) on page 1255). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying software application overviews on page 547).
Main data	Opens the **Main data – Software** page (see Main data - Software (page description) on page 1255).

Tile	Description
	Here you see the software application's main data (see Displaying software application main data on page 548).
Memberships	Opens the **Memberships – Software** page (see Memberships – Software (page description) on page 1256). Here you can see identities to which the software application is assigned (see Displaying memberships in software applications on page 548).
Attestation	Opens the **Attestation – Software** page (see Attestation – Software (page description) on page 1257). You select the following actions: • Display all attestation cases linked to this software application (see Displaying software application attestation cases on page 549) • Display identities that have yet to approve software application attestation cases (see Displaying attestors of software application pending attestation cases on page 550) • Display details of the objects being attested (see Displaying software application attestation cases on page 549)
Usage	Opens the **Usage – Software** page (see Usage – Software (page description) on page 1258). Here you can see which roles the members of the software application belong to (see Displaying role memberships of software application members on page 551).

Overview - Software (page description)

To open the **Overview – Software** page go to **Responsibilities** > **Auditing** > **Software** > **Show details** > **Overview**.

On the **Overview – Software** page, you can see all the information relevant to the software summarized in an overview (see Displaying software application overviews on page 547).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data - Software (page description)

To open the **Main data – Software** page go to **Responsibilities** > **Auditing** > **Software** > **Show details** > **Software**.

On the **Main data – Software** page, you can see the software application's main data (see Displaying software application main data on page 548).

Enter the following main data:

Table 628: Sofware application main data

Property	Description
Software name	Shows the full, descriptive name of the software application.
Version	Shows the version of the software application.
Language	Shows which language the software application uses.
Internal product name	Shows the company internal name of the software application.
Website.	Shows the URL of the manufacturer's product website.
Link to documentation	Shows the website URL containing the document.
Description	Shows the software application's description.
Comment	Shows an informative comment about the software application.
IT Shop	Shows whether the software application can be requested through IT Shop. If set, this software application can be requested by identities using the Web Portal and granted through a defined approval process. The software application can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows whether the software application can only be requested through the IT Shop. If set, this software application can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign a software application to hierarchical roles directly.
Disabled	Shows whether the software application is disabled. Only enabled software applications can be assigned in One Identity Manager. If a software application is disabled, the software cannot be assigned but any existing assignments are upheld.
Service item	Shows assigned service items.

Memberships – Software (page description)

To open the **Memberships – Software** page go to **Responsibilities** > **Auditing** > **Software** > **Show details** > **Memberships**.

On the **Memberships - Software** page, you can see identities to which the software application is assigned (see Displaying memberships in software applications on page 548).

The following table gives an overview of the different content on the **Memberships – Software** page.

Table 629: Columns

Column	Description
Identity	Shows you the name of the identity to which the software application is assigned.
Origin	Shows you whether the software application was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Software (page description)

To open the **Attestation – Software** page go to **Responsibilities** > **Auditing** > **Software** > **Show details** > **Attestation**.

On the **Attestation - Software** page, you can:

- Display all attestation cases linked to this software application (see Displaying software application attestation cases on page 549)
- Display identities that have yet to approve software application attestation cases (see Displaying attestors of software application pending attestation cases on page 550)
- Display details of the objects being attested (see Displaying software application attestation cases on page 549)

The following tables give you an overview of the various features and content on the **Attestation - Software** page.

Table 630: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of software application pending attestation cases on page 550).

Table 631: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying software application attestation cases on page 549).

Table 632: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Software (page description)

To open the **Usage - Software** page go to **Responsibilities** > **Auditing** > **Software** > **Show details** > **Usage**.

On the **Usage – Software** page, you can see the roles and organizations that belong to the identities to which this software application is assigned (see Displaying role memberships of software application members on page 551).

The following tables give you an overview of the different functions on the **Usage - Software** page.

Table 633: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Locations (page description)

Open the **Auditing - Locations** page by navigating through **Responsibilities** > **Auditing** > **Locations**.

On the **Auditing - Locations** page, you can see all the locations (see Displaying all locations on page 553).

If you click **Show details** in a location's details pane, a new page opens (see Auditing - Roles and permissions: location (page description) on page 1260) that contains more information and configuration options for the location.

The following tables give you an overview of the various features and content on the **Auditing – Locations** page.

Table 634: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the locations they manage are shown (see Displaying all locations on page 553).

Table 635: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: location** page (see Auditing - Roles and permissions: location (page description) on page 1260). Use this button to display more details about the location.

Table 636: Columns

Column	Description
Display	Shows the location's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: location (page description)

To open the **Auditing - Roles and entitlements: location** page go to **Responsibilities** > **Auditing** > **Locations** > **Show details**.

On the **Auditing - Roles and entitlements: location** page, you can access various information about the selected location.

To do this, click on one of the tiles:

Table 637: Tiles

Tile	Description
Overview	Opens the **Overview – Location** page (see Overview - Location (page description) on page 1261). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying location overviews on page 553).
Main data	Opens the **Main data – Location** page (see Main data - Location (page description) on page 1261). Here you can see the location's main data (see Displaying location main data on page 554).
Memberships	Opens the **Memberships - Location** page (see Memberships – Location (page description) on page 1262). Here you can see identities assigned to the location (see Displaying memberships in locations on page 554).
Entitlements	Opens the **Entitlements – Location** page (see Entitlements – Location (page description) on page 1263). Here you can see the entitlements assigned to the location (see Displaying location entitlements on page 555).
Attestation	Opens the **Attestation – Location** page (see Auditing– Location (page description) on page 1263). You select the following actions: • Display all attestation cases linked to this location (see Displaying location attestation cases on page 556) • Display identities that have yet to approve location attestation cases (see Displaying attestors of location pending attestation cases on page 557) • Display details of the objects being attested (see Displaying location attestation cases on page 556)
Compliance	Opens the **Compliance – Location** page (see Compliance – Location

Tile	Description
	(page description) on page 1265). Here you can show compliance rule violations that were caused by this location (see Displaying location rule violations on page 559).
Risk	Opens the **Risk – Location** page (see Risk – Location (page description) on page 1265). Here you can see the location's risk index (see Displaying location risk indexes on page 559). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – Location** page (see History – Location (page description) on page 1266). Here you can see all the changes made to the location (see Location history on page 560).
Usage	Opens the **Usage – Location** page (see Usage – Location (page description) on page 1268). Opens the **Usage – System role** page (see Usage – System role (page description) on page 1278). Here you can see which roles the members of the site belong to (see Displaying role memberships of location members on page 563).

Overview - Location (page description)

To open the **Overview – Location** page go to **Responsibilities** > **Auditing** > **Locations** > **Show details** > **Overview**.

On the **Overview - Location** page, you can see all the information relevant to the location summarized in an overview (see Displaying location overviews on page 553).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data - Location (page description)

To open the **Main data – Location** page go to **Responsibilities** > **Auditing** > **Locations** > **Show details** > **Main data**.

On the **Main data – Location** page, you can see the location's main data (see Displaying location main data on page 554).

Enter the following main data:

Table 638: Location main data

Property	Description
Location	Shows the full, descriptive name of the location.
Short name	Shows the location's short name.
Name	Shows the location's additional identifier.
Parent location	Shows the parent location of this location. If the location is at the root of a location hierarchy, the field is empty.
Attestors	Shows the attestor application role. Members of this application role can approve attestation cases for the location.
Department	Shows the department assigned to the location.
Cost center	Shows the cost center that the location is primarily assigned to.
Role approver	Shows the role approver. Members of the selected application role can approve requests for members of the location.
Role approver (IT)	Shows the IT application role approver. Members of the selected application role can approve requests for members of the location.
Manager	Shows the identity responsible for the location.
2nd Manager	Shows the identity acting as a deputy to the location's manager.
Description	Shows the location's description.

Memberships – Location (page description)

To open the **Memberships – Location** page go to **Responsibilities** > **Auditing** > **Locations** > **Show details** > **Memberships**.

On the **Memberships - Location** page, you can see identities assigned to the location (see Displaying memberships in locations on page 554).

The following table gives an overview of the different content on the **Memberships – Location** page.

Table 639: Columns

Column	Description
Identity	Shows you the name of the identity assigned to the location.
Origin	Shows you whether the location was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Location (page description)

To open the **Entitlements – Location** page go to **Responsibilities** > **Auditing** > **Locations** > **Show details** > **Entitlements**.

On the **Entitlements – Location** page, you can see the entitlements assigned to the location (see Displaying location entitlements on page 555).

The following table gives you an overview of the various features and content on the **Entitlements – application roles** page.

Table 640: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing– Location (page description)

To open the **Attestation – Location** page go to **Responsibilities** > **Auditing** > **Locations** > **Show details** > **Attestation**.

On the **Attestation - Location** page, you can:

- Display all attestation cases linked to this location (see Displaying location attestation cases on page 556)

- Display identities that have yet to approve location attestation cases (see Displaying attestors of location pending attestation cases on page 557)
- Display details of the objects being attested (see Displaying location attestation cases on page 556)

The following tables give you an overview of the various features and content on the **Attestation - Location** page.

Table 641: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of location pending attestation cases on page 557).

Table 642: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying location attestation cases on page 556).

Table 643: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Location (page description)

Open the **Compliance – Location** page by navigating through **Responsibilities** > **Auditing** > **Locations** > **Show details** > **Compliance**.

On the **Compliance – Location** page, you can see compliance rule violations connected with this location (see Displaying location rule violations on page 559).

The following table gives an overview of the content of the **Compliance – System role** page.

Table 644: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Location (page description)

To open the **Compliance – Location** page go to **Responsibilities** > **Auditing** > **Locations** > **Show details** > **Compliance**.

On the **Risk – Location** page, you can:

- Display the location's calculated risk index (see Displaying location risk indexes on page 559)

- See how the calculated risk index is put together (see Displaying location risk indexes on page 559)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – Location** page.

Table 645: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying location risk indexes on page 559).

Table 646: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Location (page description)

To open the **History – Location** page go to **Responsibilities** > **Auditing** > **Locations** > **Show details** > **History**.

On the **History – Location** page, you can see all the changes made to the location (see Location history on page 560).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a location, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you

also see all the steps in between.

- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Location** page.

Table 647: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying location history on page 560). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying location history on page 560).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying location history on page 560).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of locations on page 562).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of locations on page 562).

Table 648: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 649: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.

Column	Description
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Location (page description)

To open the **Usage – Location** page go to **Responsibilities** > **Auditing** > **Locations** > **Show details** > **Usage**.

On the **Usage – Location** page, you can see which roles and organizations belong to the identities to which this location is assigned (see Displaying role memberships of location members on page 563).

The following tables give you an overview of the different functions on the **Usage - Locations** page.

Table 650: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – System roles (page description)

Open the **Auditing - System roles** page by navigating through **Responsibilities** > **Auditing** > **System role**.

On the **Auditing - System roles** page, you can see all the system roles (see Displaying all system roles on page 564).

If you click **Show details** in a system role's details pane, a new page opens (see Auditing - Roles and permissions: system role (page description) on page 1270) that contains more information and configuration options for the system role.

The following tables give you an overview of the various features and content on the **Auditing – System roles** page.

Table 651: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the cost centers they manage are shown (see Displaying all system roles on page 564).

Table 652: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - Roles and entitlements: system role** page (see Auditing - Roles and permissions: system role (page description) on page 1270). Use this button to display more details about the system role.

Table 653: Columns

Column	Description
Display	Shows the system role's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: system role (page description)

To open the **Auditing - Roles and entitlements: system role** page go to **Responsibilities** > **Auditing** > **System roles** > **Show details**.

On the **Auditing - Roles and entitlements: system role** page, you can access various information about the selected system ole.

To do this, click on one of the tiles:

Table 654: Tiles

Tile	Description
Overview	Opens the **Overview – System role** page (see Overview – System role (page description) on page 1271). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system role overviews on page 565).
Main data	Opens the **Main data – System role** page (see Main data – System role (page description) on page 1271). Here you see the system role's main data (see Displaying system role main data on page 565).
Memberships	Opens the **Memberships – System role** page (see Memberships – System role (page description) on page 1272). Here you can see identities to which the system role is assigned (see Displaying memberships in system roles on page 566).
Entitlements	Opens the **Entitlements – System role** page (see Entitlements – System role (page description) on page 1273). Here you can see the entitlements assigned to the system role (see Displaying system role entitlements on page 567).
Attestation	Opens the **Attestation – System role** page (see Attestation – System role (page description) on page 1273). You select the following actions: • Display all attestation cases linked to this system role (see Displaying system role attestation cases on page 568) • Display identities that have yet to approve system role attestation cases (see Displaying attestors of system role pending attestation cases on page 569) • Display details of the objects being attested (see Displaying system role attestation cases on page 568)
Compliance	Opens the **Compliance – System role** page (see Compliance –

Tile	Description
	System role (page description) on page 1275). Here you can show compliance rule violations that were caused by this system role (see Displaying system role rule violations on page 571).
Risk	Opens the **Risk – System role** page (see Risk – System role (page description) on page 1275). Here you can see the system role's risk index (see Displaying system role risk indexes on page 571). For more information about risk assessment, see the Risk assessment on page 209.
History	Opens the **History – System role** page (see History – System role (page description) on page 1276). Here you can see all the changes made to the system role (see System role history on page 572).
Usage	Here you can see which roles the members of the system role belong to (see Displaying role memberships of system role members on page 575).

Overview – System role (page description)

To open the **Overview – System role** page go to **Responsibilities** > **Auditing** > **System roles** > **Show details** > **Overview**.

On the **Overview - System role** page, you can see all the information relevant to the system role in summarized in an overview (see Displaying system role overviews on page 565).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – System role (page description)

Open the **Main data – System role** page by navigating through **Responsibilities** > **Auditing** > **System roles** > **Show details** > **Main data**.

On the **Main data – System role** page, you can see the system role's main data (see Displaying system role main data on page 565).

Enter the following main data:

Table 655: System role main data

Property	Description
System role	Shows the full, descriptive name of the system role.

Property	Description
Display name	Shows the name used to display the system role in the One Identity Manager tools.
Internal product name	Shows you the company internal name of the system role.
System role type	Shows the system role's role type. The system role type specifies which type of company resources make up the system role.
System role manager	Shows the identity responsible for the system role.
Comment	Shows an informative comment about the system role.
IT Shop	Shows whether the system role can be requested in the IT Shop. If set, the system role can be requested by identities using the Web Portal and granted through a defined approval process. The system role can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows whether the system role can only be requested through the IT Shop. If set, the system role can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign a system role to hierarchical roles directly.
Service item	Shows assigned service items.

Memberships – System role (page description)

To open the **Memberships – System role** page go to **Responsibilities** > **Auditing** > **System roles** > **Show details** > **Memberships**.

On the **Memberships - System Role** page, you can see identities to which the system role is assigned (see Displaying memberships in system roles on page 566).

The following table gives an overview of the different content on the **Memberships - System role** page.

Table 656: Columns

Column	Description
Identity	Shows you the name of the identity to which the system role is assigned.
Origin	Shows you whether the system role was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – System role (page description)

To open the **Entitlements – System roles** page go to **Responsibilities** > **Auditing** > **System roles** > **Show details** > **Entitlements**.

On the **Entitlements – System role** page, you can see the entitlements assigned to the system role (see Displaying system role entitlements on page 567).

The following table gives you an overview of the various features and content on the **Entitlements – application roles** page.

Table 657: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – System role (page description)

To open the **Attestation – System roles** page go to **Responsibilities** > **Auditing** > **System roles** > **Show details** > **Attestation**.

On the **Attestation - System role** page, you can:

- Display all attestation cases linked to this system role (see Displaying system role attestation cases on page 568)

- Display identities that have yet to approve system role attestation cases (see Displaying attestors of system role pending attestation cases on page 569)
- Display details of the objects being attested (see Displaying system role attestation cases on page 568)

The following tables give you an overview of the various features and content on the **Attestation - System role** page.

Table 658: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system role pending attestation cases on page 569).

Table 659: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying system role attestation cases on page 568).

Table 660: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – System role (page description)

Open the **Compliance – System role** page by navigating through **Responsibilities** > **Auditing** > **System roles** > **Show details** > **Compliance**.

On the **Compliance – System role** page, you can see compliance rule violations connected with this system role (see Displaying system role rule violations on page 571).

The following table gives an overview of the content of the **Compliance – System role** page.

Table 661: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – System role (page description)

To open the **Compliance – System role** page go to **Responsibilities** > **Auditing** > **System roles** > **Show details** > **Compliance**.

On the **Risk – System role** page, you can:

- Display the system role's calculated risk index (see Displaying system role risk indexes on page 571)

- See how the calculated risk index is put together (see Displaying system role risk indexes on page 571)

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the different functions and content on the **Risk – System role** page.

Table 662: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index (see Displaying system role risk indexes on page 571).

Table 663: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – System role (page description)

To open the **History – System role** page go to **Responsibilities** > **Auditing** > **System roles** > **Show details** > **History**.

On the **History – System role** page, you can see all the changes made to the system role (see System role history on page 572).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system role, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you

also see all the steps in between.

- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – System role** page.

Table 664: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system role history on page 572). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system role history on page 572).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system role history on page 572).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system roles on page 574).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system roles on page 574).

Table 665: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 666: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.

Column	Description
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – System role (page description)

To open the **Usage – System role** page go to **Responsibilities** > **Auditing** > **System roles** > **Show details** > **Usage**.

On the **Usage – System role** page, you can see the roles and organizations that belong to the identities to which this system role is assigned (see Displaying role memberships of system role members on page 575).

The following tables give you an overview of the different functions on the **Usage - System roles** page.

Table 667: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing - Assignment resource (page description)

Open the **Auditing - Assignment resources** page by navigating through **Responsibilities** > **Auditing** > **Assignment resources**.

On the **Auditing - Assignment resources** page, you can see all the assignment resources (see Displaying all assignment resources on page 585).

If you click **Show details** in an assignment resource's details pane, a new page opens (see Auditing - Roles and entitlements: assignment resource (page description) on page 1280) that contains more information and configuration options for the assignment resource.

The following tables give you an overview of the various features and content on the **Auditing – Assignment resources** page.

Table 668: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the assignment resources they manage are shown (see Displaying all assignment resources on page 585).

Table 669: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: assignment resource** page (see Auditing - Roles and entitlements: assignment resource (page description) on page 1280). Use this button to display more details about the assignment resource.

Table 670: Columns

Column	Description
Display	Shows the assignment resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and entitlements: assignment resource (page description)

To open the **Auditing - Roles and entitlements: assignment resource** page go to **Responsibilities** > **Auditing** > **Assignment resources** > **Show details**.

On the **Auditing - Roles and entitlements: assignment resource** page, you can access various information about the selected assignment resource.

To do this, click on one of the tiles:

Table 671: Tiles

Tile	Description
Overview	Opens the **Overview – Assignment resource** page (see Overview – Assignment resource (page description) on page 1280). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying assignment resource overviews on page 586).
Main data	Opens the **Main data – Assignment resource** page (see Main data – Assignment resource (page description) on page 1281). Here you see the assignment resource's main data (see Displaying assignment resource main data on page 586).
Attestation	Opens the **Attestation – Assignment resource** page (see Attestation - Assignment resource (page description) on page 1281). You select the following actions: • Display all attestation cases linked to this assignment resource (see Displaying assignment resource attestation cases on page 587) • Display identities that have yet to approve assignment resource attestation cases (see Displaying attestors of assignment resource pending attestation cases on page 588) • Display details of the objects being attested

Overview – Assignment resource (page description)

To open the **Overview – Assignment resource** page go to **Responsibilities** > **Auditing** > **Assignment resources** > **Show details** > **Overview**.

On the **Overview - Assignment resource** page, you can see all the information relevant to the assignment resource summarized in an overview (see Displaying assignment resource overviews on page 586).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Assignment resource (page description)

Open the **Main data – Assignment resource** page by navigating through **Responsibilities** > **Auditing** > **Assignment resources** > **Show details** > **Main data**.

On the **Main data – Assignment resource** page, you can see the assignment resource's main data (see Displaying assignment resource main data on page 586).

Enter the following main data:

Table 672: Assignment resource main data

Property	Description
Assignment resource	Shows the full, descriptive name of the assignment resource.
Resource type	Shows the type of resource. Use resource types to group assignment resources.
Description	Shows the assignment resource's description.
IT Shop	Shows whether the assignment resource can be requested through the IT Shop. If set, this assignment resource can be requested by identities using the Web Portal and granted through a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows whether the assignment resource can only be requested through the IT Shop. If set, this assignment resource can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign an assignment resource to hierarchical roles directly.
Service item	Shows assigned service items.
Risk index	Shows the configured risk index. This value specifies the risk of assigning this multi-request assignment resource to an identity.
Requested assignments remain intact.	Shows whether the organization/business role resource requested by an identity remain intact if the identity loses their entitlement to make requests.

Attestation - Assignment resource (page description)

To open the **Attestation – Assignment resource** page go to **Responsibilities** > **Auditing** > **Assignment resources** > **Show details** > **Attestation**.

On the **Attestation - Assignment resource** page, you can:

- Display all attestation cases linked to this assignment resource (see Displaying assignment resource attestation cases on page 587)
- Display identities that have yet to approve assignment resource attestation cases (see Displaying attestors of assignment resource pending attestation cases on page 588)
- Display details of the objects being attested

The following tables give you an overview of the various features and content on the **Attestation - Assignment resource** page.

Table 673: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities .

Table 674: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case .

Table 675: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.

Column	Description
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing – Active Directory (page description)

To open the **Auditing - Active Directory** page go to **Responsibilities** > **Auditing** > **Active Directory**.

On the **Auditing -** page, you can see all the Active Directory groups (see Active Directory).Displaying all system entitlements on page 576

If you click **Show details** in an Active Directory group's details pane, a new page opens (see Auditing - Roles and permissions: Active Directory group (page description) on page 1284) that contains more information and configuration options for the Active Directory group.

The following tables give you an overview of the various features and content on the **Auditing - Active Directory** page.

Table 676: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the Active Directory groups they manage are shown (see Displaying all system entitlements on page 576).

Table 677: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: Active Directory group** page (see Auditing - Roles and permissions: Active Directory group (page description) on page 1284). Use this button to display more details about the Active Directory group.

Table 678: Columns

Column	Description
Display	Shows the Active Directory group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: Active Directory group (page description)

To open the **Auditing - Roles and entitlements: Active Directory group** page go to **Responsibilities** > **Auditing** > **Active Directory** > **Show details.**

On the **Auditing - Roles and entitlements: Active Directory group** page, you can access various information about the selected Active Directory group.

To do this, click on one of the tiles:

Table 679: Tiles

Tile	Description
Overview	Opens the **Overview – Overview – Active Directory group (page description) on page 1285 group** page (see Active Directory). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – Active Directory group** (see Main data – Active Directory group (page description) on page 1285). Here you can see the Active Directory group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – Active Directory group** page (see Memberships – Active Directory group (page description) on page 1286). Here you can see identities to which the Active Directory group is assigned (see Displaying memberships in system entitlements on page 578).
Child groups	Opens the **Child groups – Active Directory group** (see Child groups – Active Directory group (page description) on page 1288). You can select the following actions: • Display child groups of the Active Directory group (see Displaying system entitlement child groups on page 578)
Attestation	Opens the **Attestation – Active Directory group** (see Attestations – Active Directory group (page description) on page 1287). You select the following actions: • Display all attestation cases linked to this Active Directory group (see Displaying attestation cases of system entitlements on page 579)

Tile	Description
	• Display identities that have yet to approve Active Directory group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)
History	Opens the **History – Active Directory group** page (see History – Active Directory group (page description) on page 1288). Here you can see all the changes made to the Active Directory group (see System entitlement history on page 581).
Usage	Opens the **Usage – Active Directory group** page (see Usage – Active Directory group (page description) on page 1291). Here you can see which roles the members of the Active Directory group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – Active Directory group (page description)

To open the **Overview - Active Directory group** page go to **Responsibilities** > **Auditing** > **Active Directory** > **Show details** > **Overview**.

On the **Overview – Active Directory group** page, you can see all the information relevant to the Active Directory group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Active Directory group (page description)

To open the **Main data – Active Directory group** page go to **Responsibilities** > **Auditing** > **Active Directory** > **Show details** > **Main data**.

On the **Main data – Active Directory group** page, you can see the Active Directory group's main data (see Displaying system entitlement main data on page 577).

Enter the following main data:

Table 680: Active Directory group main data

Property	Description
Name	Shows you the full, descriptive name of the Active Directory group.
Canonical name	Shows you the automatically generated canonical name of the Active Directory group.
Distinguished name	Shows you the automatically generated distinguished name of the Active Directory group.

Property	Description
Display name	Shows you the name of the Active Directory group used to display Active Directory group in the One Identity Manager tools.
Container	Shows you the parent container of the Active Directory group.
Service item	Shows you the assigned service items.
Category	Shows you the category for Active Directory group inheritance. User accounts can inherit Active Directory groups selectively. To do this, Active Directory groups and user accounts are divided into categories.
Description	Shows you the Active Directory group's description.
Risk index	Shows you the configured risk index. This value specifies the risk of assigning this Active Directory group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the Active Directory group can be requested in the IT Shop. If set, the Active Directory group can be requested by identities using the Web Portal and granted through a defined approval process. The Active Directory group can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows you whether the Active Directory group can only be requested through the IT Shop. If set, the Active Directory group can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign an Active Directory group to hierarchical roles directly.

Memberships – Active Directory group (page description)

To open the **Memberships – Active Directory group** page go to **Responsibilities** > **Auditing** > **Active Directory** > **Show details** > **Memberships**.

On the **Memberships - Active Directory group** page, you can see identities to which the Active Directory group is assigned.

The following table gives an overview of the different content on the **Memberships – Active Directory group** page.

Table 681: Columns

Column	Description
Identity	Shows you the name of the identity to which the Active Directory group is assigned.

Column	Description
Origin	Shows whether the Active Directory group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – Active Directory group (page description)

To open the **Attestation – Active Directory group** page go to **Responsibilities** > **Auditing** > **Active Directory** > **Show details** > **Attestation**.

On the **Attestation - Active Directory group** page, you can:

- Display all attestation cases linked to this Active Directory group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve Active Directory group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the various features and content on the **Attestation - Active Directory group** page.

Table 682: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 683: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 684: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Child groups – Active Directory group (page description)

To open the **Compliance - Active Directory group** page go to **Responsibilities** > **Auditing** > **Active Directory** > **Show details** > **Compliance**.

On the **Compliance - Active Directory group** page, you can see all the child groups of the Active Directory group (see Displaying system entitlement child groups on page 578).

History – Active Directory group (page description)

To open the **History – Active Directory group** page go to **Responsibilities** > **Auditing** > **Active Directory** > **Show details** > **History**.

On the **History – Active Directory group** page, you can see all the changes made to the Active Directory group (see System entitlement history on page 581).

| NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Active Directory** page.

Table 685: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 686: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 687: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Active Directory group (page description)

To open the **Usage – Active Directory group** page go to **Responsibilities** > **Auditing** > **Active Directory** > **Show details** > **Usage**.

On the **Usage – Active Directory group** page, you can see the roles and organizations that belong to the identities to which the Active Directory group is assigned (see Displaying role memberships of system entitlement members on page 584).

The following tables give you an overview of the different functions on the **Usage - Active Directory** page.

Table 688: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Azure Active Directory (page description)

To open the **Auditing - Azure Active Directory** page go to **Responsibilities** > **Auditing** > **Azure Active Directory**.

On the **Auditing - Azure Active Directory** page, you can see all the Azure Active Directory groups (see Displaying all system entitlements on page 576).

If you click **Show details** in an Azure Active Directory group's details pane, a new page opens (see Auditing - Roles and permissions: Azure Active Directory group (page description) on page 1292) that contains more information and configuration options for the Azure Active Directory group.

The following tables give you an overview of the various features and content on the **Auditing - Azure Active Directory** page.

Table 689: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the Azure Active Directory groups they manage are shown (see Displaying all system entitlements on page 576).

Table 690: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: Azure Active Directory group** page (see Auditing - Roles and permissions: Azure Active Directory group (page description) on page 1292). Use this button to display more details about the Azure Active Directory group.

Table 691: Columns

Column	Description
Display	Shows the Azure Active Directory group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: Azure Active Directory group (page description)

To open the **Auditing - Roles and entitlements: Azure Active Directory group** page go to **Responsibilities** > **Auditing** > **Azure Active Directory** > **Show details**.

On the **Auditing - Roles and entitlements: Azure Active Directory group** page, you can access various information about the selected Azure Active Directory group.

To do this, click on one of the tiles:

Table 692: Tiles

Tile	Description
Overview	Opens the **Overview – Overview – Azure Active Directory group (page description) on page 1293 group** page (see Azure Active Directory). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – Azure Active Directory group** (see Main data – Azure Active Directory group (page description) on page 1293). Here you can see the Azure Active Directory group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – Azure Active Directory group** page (see Memberships – Azure Active Directory group (page description) on page 1294).

Tile	Description
	Here you can see identities to which the Azure Active Directory group is assigned (see Displaying memberships in system entitlements on page 578).
Attestation	Opens the **Attestation – Azure Active Directory group** (see Attestations – Azure Active Directory group (page description) on page 1295). You select the following actions: • Display all attestation cases linked to this Azure Active Directory group (see Displaying attestation cases of system entitlements on page 579) • Display identities that have yet to approve Azure Active Directory group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)
History	Opens the **History – Azure Active Directory group** page (see History – Azure Active Directory group (page description) on page 1297). Here you can see all the changes made to the Azure Active Directory group (see System entitlement history on page 581).
Usage	Opens the **Usage – Azure Active Directory group** page (see Usage – Azure Active Directory group (page description) on page 1299). Here you can see which roles the members of the Azure Active Directory group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – Azure Active Directory group (page description)

To open the **Overview - Azure Active Directory group** page go to **Responsibilities** > **Auditing** > **Azure Active Directory** > **Show details** > **Overview**.

On the **Overview – Azure Active Directory group** page, you can see all the information relevant to the Azure Active Directory group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Azure Active Directory group (page description)

To open the **Main data – Azure Active Directory group** page go to **Responsibilities** > **Auditing** > **Azure Active Directory** > **Show details** > **Main data**.

On the **Main data – Azure Active Directory group** page, you can see the Azure Active Directory group's main data (see Displaying system entitlement main data on page 577).

Enter the following main data:

Table 693: Azure Active Directory group main data

Property	Description
Name	Shows you the full, descriptive name of the Azure Active Directory group.
Canonical name	Shows you the automatically generated canonical name of the Azure Active Directory group.
Distinguished name	Shows you the automatically generated distinguished name of the Azure Active Directory group.
Display name	Shows you the name of the Azure Active Directory group used to display Azure Active Directory group in the One Identity Manager tools.
Container	Shows you the parent container of the Azure Active Directory group.
Service item	Shows you the assigned service items.
Category	Shows you the category for Azure Active Directory group inheritance. User accounts can inherit Azure Active Directory groups selectively. To do this, Azure Active Directory groups and user accounts are divided into categories.
Description	Shows you the Azure Active Directory group's description.
Risk index	Shows you the configured risk index. This value specifies the risk of assigning this Azure Active Directory group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the Azure Active Directory group can be requested in the IT Shop. If set, the Azure Active Directory group can be requested by identities using the Web Portal and granted through a defined approval process. The Azure Active Directory group can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows you whether the Azure Active Directory group can only be requested through the IT Shop. If set, the Azure Active Directory group can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign an Azure Active Directory group to hierarchical roles directly.

Memberships – Azure Active Directory group (page description)

To open the **Memberships – Azure Active Directory group** page go to **Responsibilities** > **Auditing** > **Azure Active Directory** > **Show details** >

Memberships.

On the **Memberships - Azure Active Directory group** page, you can see identities to which the Azure Active Directory group is assigned (see Displaying memberships in system entitlements on page 578).

The following table gives an overview of the different content on the **Memberships – Azure Active Directory group** page.

Table 694: Columns

Column	Description
Identity	Shows you the name of the identity to which the Azure Active Directory group is assigned.
Origin	Shows whether the Azure Active Directory group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – Azure Active Directory group (page description)

To open the **Attestation – Azure Active Directory group** page go to **Responsibilities** > **Auditing** > **Azure Active Directory** > **Show details** > **Attestation**.

On the **Attestation - Azure Active Directory group** page, you can:

- Display all attestation cases linked to this Azure Active Directory group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve Azure Active Directory group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the various features and content on the **Attestation - Azure Active Directory group** page.

Table 695: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 696: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 697: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

History – Azure Active Directory group (page description)

To open the **History – Azure Active Directory group** page go to **Responsibilities** > **Auditing** > **Azure Active Directory** > **Show details** > **History**.

On the **History – Azure Active Directory group** page, you can see all the changes made to the Azure Active Directory group (see System entitlement history on page 581).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.
- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Azure Active Directory** page.

Table 698: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 699: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 700: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Azure Active Directory group (page description)

To open the **Usage – Azure Active Directory group** page go to **Responsibilities** > **Auditing** > **Azure Active Directory** > **Show details** > **Usage**.

On the **Usage – Azure Active Directory group** page, you can see the roles and organizations that belong to the identities to which the Azure Active Directory group is assigned (see Displaying role memberships of system entitlement members on page 584).

The following tables give you an overview of the different functions on the **Usage - Azure Active Directory** page.

Table 701: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Custom target system group (page description)

Open the **Auditing - Custom target systems** page by navigating through **Responsibilities** > **Auditing** > **Custom target systems**.

On the **Auditing - Custom target system** page, you can see all the custom target systems groups (see Displaying all system entitlements on page 576).

If you click **Show details** in a custom target system's details pane, a new page opens (see Auditing - Roles and entitlements: custom target system group (page description) on page 1300) that contains more information and configuration options for the custom target system group.

The following tables give you an overview of the various features and content on the **Auditing – custom target systems** page.

Table 702: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the custom target system groups they manage are shown (see Displaying all system entitlements on page 576).

Table 703: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: custom target system group** page (see Auditing - Roles and entitlements: custom target system group (page description) on page 1300). Use this button to display more details about the custom target system group.

Table 704: Columns

Column	Description
Display	Shows the custom target system group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and entitlements: custom target system group (page description)

To open the **Auditing - Roles and entitlements: Custom target system group** page go to **Responsibilities** > **Auditing** > **Custom target systems** > **Show details**.

On the **Auditing - Roles and entitlements: custom target system group** page, you can access various information about the selected assignment custom target system group.

To do this, click on one of the tiles:

Table 705: Tiles

Tile	Description
Overview	Opens the **Overview – Custom target system group** page (see Overview – Custom target system group (page description) on page 1301). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – Custom target system group** (see Main data – Custom target system group (page description) on page 1302). Here you see the custom target system group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – Custom target system group** (see Memberships – Custom target system group (page description) on page 1303).

Tile	Description
	Here you can see identities to which the group of the custom target system is assigned (see Displaying memberships in system entitlements on page 578).
Child groups	Opens the **Child groups – Custom target system group** (see Child groups – Custom target system group (page description) on page 1305). You can select the following actions: • Display child groups of the custom target system group (see Displaying system entitlement child groups on page 578)
Attestation	Opens the **Attestation – Custom target system group** (see Attestations – Custom target system group (page description) on page 1303). You select the following actions: • Display all attestation cases linked to this custom target system group (see Displaying attestation cases of system entitlements on page 579) • Display identities that have yet to approve custom target system resource attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)
History	Opens the **History – Custom target system group** (see History – Custom target system group (page description) on page 1305). Here you can see all the changes made to the custom target system group (see System entitlement history on page 581).
Usage	Opens the **Usage – Custom target system group** page (see Usage – Custom target system group (page description) on page 1307). Here you can display which roles the members of the custom target system group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – Custom target system group (page description)

To open the **Overview – Custom target system group** page go to **Responsibilities** > **Auditing** > **Custom target systems** > **Show details** > **Overview**.

On the **Overview – Custom target system group** page, you can see all the information relevant to the custom target system group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Custom target system group (page description)

Open the **Main data – custom target system group** page by navigating through **Responsibilities** > **Auditing** > **custom target systems** > **Show details** > **Main data**.

On the **Main data – Custom target system group** page, you can see the custom target system group's main data (see Displaying system entitlement main data on page 577).

Enter the following main data:

Table 706: Custom target system group main data

Property	Description
Name	Shows you the full, descriptive name of the custom target system group.
Canonical name	Shows you the automatically generated canonical name of the custom target system.
Distinguished name	Shows you the automatically generated distinguished name of the custom target system.
Display name	Shows you the name of the custom target system group used to display the custom target system in the One Identity Manager tools.
Container	Shows you the parent container of the custom target system group.
Service item	Shows you the assigned service items.
Category	Shows you the category for custom target system group inheritance. User accounts can inherit custom target system groups selectively. To do this, custom target system groups and user accounts are divided into categories.
Description	Shows you the custom target system group's description.
Risk index	Shows you the configured risk index. This value specifies the risk of assigning this custom target system group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the custom target system group can be requested in the IT Shop. If set, the custom target system group can be requested by identities using the Web Portal and granted through a defined approval process. The custom target system group can still be assigned to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows you whether the custom target system group can only be requested in the IT Shop. If set, the custom target system group can be

Property	Description
	requested by identities using the Web Portal and granted through a defined approval process. You cannot assign a custom target system group to hierarchical roles directly.

Memberships – Custom target system group (page description)

To open the **Memberships – Custom target system group** page, navigate to **Responsibilities** > **Auditing** > **Custom target system** > **Show details** > **Memberships**.

On the **Memberships - Custom target system group** page, you can see identities to which the customer target system group is assigned (see Displaying memberships in system entitlements on page 578).

The following table gives an overview of the different content on the **Memberships - Custom target system group** page.

Table 707: Columns

Column	Description
Identity	Shows you the name of the identity to which the custom target system group is assigned.
Origin	Shows whether the custom target system group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – Custom target system group (page description)

To open the **Attestation – custom target system group** page go to **Responsibilities** > **Auditing** > **custom target systems** > **Show details** > **Attestation**.

On the **Attestation - Custom target system group** page, you can:

- Display all attestation cases linked to this custom target system group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve custom target system resource attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the different functions and content on the **Attestation - custom target systems** page.

Table 708: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 709: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 710: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.

Column	Description
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Child groups – Custom target system group (page description)

To open the **Compliance - custom target system group** page, navigate to **Responsibilities** > **Auditing** > **Custom target system** > **Show details** > **Compliance**.

On the **Compliance - Custom target system group** page, you can see all child groups of the custom target system group (see Displaying system entitlement child groups on page 578).

History – Custom target system group (page description)

To open the **History - Custom target system group** page, navigate to **Responsibilities** > **Auditing** > **Custom target system** > **Show details** > **History**.

On the **History – Custom target system group** page, you can see all the changes made to the custom target system group (see System entitlement history on page 581.)

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – custom target system group** page.

Table 711: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 712: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 713: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.

Column	Description
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Custom target system group (page description)

To open the **Usage – Custom target system group** page go to **Responsibilities** > **Auditing** > **Custom target systems** > **Show details** > **Usage**.

On the **Usage – Custom Target System Group** page, you can see the roles and organizations that belong to the identities to which the custom target system group is assigned belong (see Displaying role memberships of system entitlement members on page 584).

The following tables give you an overview of the different functions on the **Usage - Custom target system group**.

Table 714: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Google Workspace (page description)

To open the **Auditing - Google Workspace** page go to **Responsibilities** > **Auditing** > **Google Workspace**.

On the **Auditing - Google Workspace** page, you can see all the Google Workspace groups (see Displaying all system entitlements on page 576).

If you click **Show details** in a Google Workspace group's details pane, a new page opens (see Auditing - Roles and permissions: Google Workspace group (page description) on page 1308) that contains more information and configuration options for the Google Workspace group.

The following tables give you an overview of the various features and content on the **Auditing - Google Workspace** page.

Table 715: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the Google Workspace groups they manage are shown (see Displaying all system entitlements on page 576).

Table 716: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: Google Workspace group** page (see Auditing - Roles and permissions: Google Workspace group (page description) on page 1308). Use this button to display more details about the Google Workspace group.

Table 717: Columns

Column	Description
Display	Shows the Google Workspace group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: Google Workspace group (page description)

To open the **Auditing - Roles and entitlements: Google Workspace group** page go to **Responsibilities** > **Auditing** > **Google Workspace** > **Show details**.

On the **Auditing - Roles and entitlements: Google Workspace group** page, you can access various information about the selected Google Workspace group.

To do this, click on one of the tiles:

Table 718: Tiles

Tile	Description
Overview	Opens the **Overview – Overview – Google Workspace group (page description) on page 1310 group** page (see Google Workspace). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – Google Workspace group** (see Main data – Google Workspace group (page description) on page 1310). Here you can see the Google Workspace group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – Google Workspace group** page (see Memberships – Google Workspace group (page description) on page 1311). Here you can see identities to which the Google Workspace group is assigned (see Displaying memberships in system entitlements on page 578).
Attestation	Opens the **Attestation – Google Workspace group** (see Attestations – Google Workspace group (page description) on page 1312). You select the following actions: • Display all attestation cases linked to this Google Workspace group (see Displaying attestation cases of system entitlements on page 579) • Display identities that have yet to approve Google Workspace group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)
History	Opens the **History – Google Workspace group** page (see History – Google Workspace group (page description) on page 1313). Here you can see all the changes made to the Google Workspace group (see System entitlement history on page 581).
Usage	Opens the **Usage – Google Workspace group** page (see Usage – Google Workspace group (page description) on page 1315). Here you can see which roles the members of the Google Workspace

Tile	Description
	group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – Google Workspace group (page description)

To open the **Overview - Google Workspace group** page go to **Responsibilities** > **Auditing** > **Google Workspace** > **Show details** > **Overview**.

On the **Overview – Google Workspace group** page, you can see all the information relevant to the Google Workspace group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Google Workspace group (page description)

To open the **Main data – Google Workspace group** page go to **Responsibilities** > **Auditing** > **Google Workspace** > **Show details** > **Main data**.

On the **Main data – Google Workspace group** page, you can see the Google Workspace group's main data (see Displaying system entitlement main data on page 577).

Enter the following main data:

Table 719: Google Workspace group main data

Property	Description
Name	Shows you the full, descriptive name of the Google Workspace group.
Canonical name	Shows you the automatically generated canonical name of the Google Workspace group.
Distinguished name	Shows you the automatically generated distinguished name of the Google Workspace group.
Display name	Shows you the name of the Google Workspace group used to display Google Workspace group in the One Identity Manager tools.
Container	Shows you the parent container of the Google Workspace group.
Service item	Shows you the assigned service items.
Category	Shows you the category for Google Workspace group inheritance. User accounts can inherit Google Workspace groups selectively. To do this, Google Workspace groups and user accounts are divided into categories.
Description	Shows you the Google Workspace group's description.
Risk index	Shows you the configured risk index.

Property	Description
	This value specifies the risk of assigning this Google Workspace group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the Google Workspace group can be requested in the IT Shop. If set, the Google Workspace group can be requested by identities using the Web Portal and granted through a defined approval process. The Google Workspace group can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows you whether the Google Workspace group can only be requested through the IT Shop. If set, the Google Workspace group can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign a Google Workspace group to hierarchical roles directly.

Memberships – Google Workspace group (page description)

To open the **Memberships – Google Workspace group** page go to **Responsibilities** > **Auditing** > **Google Workspace** > **Show details** > **Memberships**.

On the **Memberships - Google Workspace group** page, you can see identities to which the Google Workspace group is assigned (see Displaying memberships in system entitlements on page 578).

The following table gives an overview of the different content on the **Memberships – Google Workspace group** page.

Table 720: Columns

Column	Description
Identity	Shows you the name of the identity to which the Google Workspace group is assigned.
Origin	Shows whether the Google Workspace group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.

- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – Google Workspace group (page description)

To open the **Attestation – Google Workspace group** page go to **Responsibilities** > **Auditing** > **Google Workspace** > **Show details** > **Attestation**.

On the **Attestation - Google Workspace group** page, you can:

- Display all attestation cases linked to this Google Workspace group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve Google Workspace group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the various features and content on the **Attestation - Google Workspace group** page.

Table 721: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 722: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 723: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.

Column	Description
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

History – Google Workspace group (page description)

To open the **History – Google Workspace group** page go to **Responsibilities** > **Auditing** > **Google Workspace** > **Show details** > **History**.

On the **History – Google Workspace group** page, you can see all the changes made to the Google Workspace group (see System entitlement history on page 581).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from

then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Google Workspace** page.

Table 724: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 725: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 726: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.

Column	Description
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Google Workspace group (page description)

To open the **Usage – Google Workspace group** page go to **Responsibilities** > **Auditing** > **Google Workspace** > **Show details** > **Usage**.

On the **Usage – Google Workspace group** page, you can see the roles and organizations that belong to the identities to which the Google Workspace group is assigned (see Displaying role memberships of system entitlement members on page 584).

The following tables give you an overview of the different functions on the **Usage - Google Workspace** page.

Table 727: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what

Control	Description
	you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Domino (page description)

Open the **Auditing - Domino** page by navigating through **Responsibilities** > **Auditing** > **Domino**.

On the **Auditing - Domino** page, you can see all the Notes groups (see Displaying all system entitlements on page 576).

If you click **Show details** in a Notes group's details pane, a new page opens (see Auditing - Roles and permissions: Notes group (page description) on page 1317) that contains more information and configuration options for the Notes group.

The following tables give you an overview of the various features and content on the **Auditing - Domino** page.

Table 728: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the Notes groups they manage are shown (see Displaying all system entitlements on page 576).

Table 729: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: Notes group** page (see Auditing - Roles and permissions: Notes group (page description) on page 1317). Use this button to display more details about the Notes group.

Table 730: Columns

Column	Description
Display	Shows the Notes group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: Notes group (page description)

To open the **Auditing - Roles and entitlements: Notes group** page go to **Responsibilities** > **Auditing** > **Domino** > **Show details**.

On the **Auditing - Roles and entitlements: Notes group** page, you can access various information about the selected Notes group.

To do this, click on one of the tiles:

Table 731: Tiles

Tile	Description
Overview	Opens the **Overview – Overview – Notes group (page description) on page 1318 group** page (see Notes). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – Notes group** (see Main data – Notes group (page description) on page 1318). Here you can see the Notes group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – Notes group** page (see Memberships – Notes group (page description) on page 1319). Here you can see identities to which the Notes group is assigned (see Displaying memberships in system entitlements on page 578).
Child groups	Opens the **Child groups – Notes group** (see Child groups – Notes group (page description) on page 1321). You can select the following actions: • Display child groups of the Notes group (see Displaying system entitlement child groups on page 578)
Attestation	Opens the **Attestation – Notes group** (see Attestations – Notes group (page description) on page 1320). You select the following actions: • Display all attestation cases linked to this Notes group (see Displaying attestation cases of system entitlements on page 579) • Display identities that have yet to approve Notes group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

Tile	Description
History	Opens the **History – Notes group** page (see History – Notes group (page description) on page 1321). Here you can see all the changes made to the Notes group (see System entitlement history on page 581).
Usage	Opens the **Usage – Notes group** page (see Usage – Notes group (page description) on page 1323). Here you can see which roles the members of the Notes group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – Notes group (page description)

To open the **Overview - Notes group** page go to **Responsibilities** > **Auditing** > **Domino** > **Show details** > **Overview**.

On the **Overview – Notes group** page, you can see all the information relevant to the Notes group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Notes group (page description)

To open the **Main data – Notes group** page go to **Responsibilities** > **Auditing** > **Domino** > **Show details** > **Main data**.

On the **Main data – Notes group** page, you can see the Notes group's main data (see Displaying system entitlement main data on page 577).

Enter the following main data:

Table 732: Notes group main data

Property	Description
Name	Shows you the full, descriptive name of the Notes group.
Canonical name	Shows you the automatically generated canonical name of the Notes group.
Distinguished name	Shows you the automatically generated distinguished name of the Notes group.
Display name	Shows you the name of the Notes group used to display Notes group in the One Identity Manager tools.
Container	Shows you the parent container of the Notes group.

Property	Description
Service item	Shows you the assigned service items.
Category	Shows you the category for Notes group inheritance. User accounts can inherit Notes groups selectively. To do this, Notes groups and user accounts are divided into categories.
Description	Shows you the Notes group's description.
Risk index	Shows you the configured risk index. This value specifies the risk of assigning this Notes group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the Notes group can be requested in the IT Shop. If set, the Notes group can be requested by identities using the Web Portal and granted through a defined approval process. The Notes group can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows you whether the Notes group can only be requested through the IT Shop. If set, the Notes group can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign a Notes group to hierarchical roles directly.

Memberships – Notes group (page description)

To open the **Memberships – Notes group** page go to **Responsibilities** > **Auditing** > **Domino** > **Show details** > **Memberships**.

On the **Memberships - Notes group** page, you can see identities to which the Notes group is assigned (see Displaying memberships in system entitlements on page 578).

The following table gives an overview of the different content on the **Memberships – Notes group** page.

Table 733: Columns

Column	Description
Identity	Shows you the name of the identity to which the Notes group is assigned.
Origin	Shows whether the Notes group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – Notes group (page description)

To open the **Attestation – Notes group** page go to **Responsibilities** > **Auditing** > **Domino** > **Show details** > **Attestation**.

On the **Attestation – Notes group** page, you can:

- Display all attestation cases linked to this Notes group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve Notes group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the various features and content on the **Attestation - Notes group** page.

Table 734: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 735: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 736: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Child groups – Notes group (page description)

To open the **Compliance - Notes group** page, navigate to **Responsibilities** > **Auditing** > **Domino** > **Show details** > **Compliance**.

On the **Compliance - Notes group** page, you can see all the child groups of the Notes group (see Displaying system entitlement child groups on page 578).

History – Notes group (page description)

To open the **History – Notes group** page go to **Responsibilities** > **Auditing** > **Domino** > **Show details** > **History**.

On the **History – Notes group** page, you can see all the changes made to the Notes group (see System entitlement history on page 581).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Domino** page.

Table 737: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 738: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of

Control	Description
	the property was at the selected point in time and what the value is now.

Table 739: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Notes group (page description)

To open the **Usage – Notes group** page go to **Responsibilities** > **Auditing** > **Domino** > **Show details** > **Usage**.

On the **Usage - Notes group** page, you can see the roles that belong to the identities to which the Notes group is assigned (see Displaying role memberships of system entitlement members on page 584).

The following table gives an overview of the different functions on the **Usage - Domino** page.

Table 740: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – LDAP (page description)

To open the **Auditing - LDAP** page go to **Responsibilities** > **Auditing** > **LDAP**.

On the **Auditing - LDAP** page, you can see all the LDAP groups (see Displaying all system entitlements on page 576).

If you click **Show details** in an LDAP group's details pane, a new page opens (see Auditing - Roles and permissions: LDAP group (page description) on page 1325) that contains more information and configuration options for the LDAP group.

The following tables give you an overview of the various features and content on the **Auditing - LDAP** page.

Table 741: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the LDAP groups they manage are shown (see Displaying all system entitlements on page 576).

Table 742: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: LDAP group** page (see Auditing - Roles and permissions: LDAP group (page description) on page 1325). Use this button to display more details about the LDAP group.

Table 743: Columns

Column	Description
Display	Shows the LDAP group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: LDAP group (page description)

To open the **Auditing - Roles and entitlements: LDAP group** page go to **Responsibilities** > **Auditing** > **LDAP** > **Show details**.

On the **Auditing - Roles and entitlements: LDAP group** page, you can access various information about the selected LDAP group.

To do this, click on one of the tiles:

Table 744: Tiles

Tile	Description
Overview	Opens the **Overview – Overview – LDAP group (page description) on page 1326 group** page (see LDAP). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – LDAP group** (see Main data – LDAP group (page description) on page 1326). Here you can see and edit the LDAP group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – LDAP group** page (see Memberships – LDAP group (page description) on page 1327). Here you can see identities to which the LDAP group is assigned (see Displaying memberships in system entitlements on page 578).
Child groups	Opens the **Child groups – LDAP group** (see Child groups – LDAP group (page description) on page 1329). You can select the following actions: • Display child groups of the LDAP group (see Displaying system entitlement child groups on page 578)
Attestation	Opens the **Attestation – LDAP group** (see Attestations – LDAP group (page description) on page 1328).

Tile	Description
	You select the following actions: • Display all attestation cases linked to this LDAP group (see Displaying attestation cases of system entitlements on page 579) • Display identities that have yet to approve LDAP group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)
History	Opens the **History – LDAP group** page (see History – LDAP group (page description) on page 1329). Here you can see all the changes made to the LDAP group (see System entitlement history on page 581).
Usage	Opens the **Usage – LDAP group** page (see Usage – LDAP group (page description) on page 1332). Here you can see which roles the members of the LDAP group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – LDAP group (page description)

To open the **Overview - LDAP group** page go to **Responsibilities** > **Auditing** > **LDAP** > **Show details** > **Overview**.

On the **Overview – LDAP group** page, you can see all the information relevant to the LDAP group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – LDAP group (page description)

To open the **Main data – LDAP group** page go to **Responsibilities** > **Auditing** > **LDAP** > **Show details** > **Main data**.

On the **Main data – LDAP group** page, you can show the LDAP group's main data.

Enter the following main data:

Table 745: LDAP group main data

Property	Description
Name	Shows you the full, descriptive name of the LDAP group.
Canonical	Shows you the automatically generated canonical name of the LDAP

Property	Description
name	group.
Distinguished name	Shows you the automatically generated distinguished name of the LDAP group.
Display name	Shows you the name of the LDAP group used to display LDAP group in the One Identity Manager tools.
Container	Shows you the parent container of the LDAP group.
Service item	Shows you the assigned service items.
Category	Shows you the category for LDAP group inheritance. User accounts can inherit LDAP groups selectively. To do this, LDAP groups and user accounts are divided into categories.
Description	Shows you the LDAP group's description.
Risk index	Shows you the configured risk index. This value specifies the risk of assigning this LDAP group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the LDAP group can be requested in the IT Shop. If set, the LDAP group can be requested by identities using the Web Portal and granted through a defined approval process. The LDAP group can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows you whether the LDAP group can only be requested through the IT Shop. If set, the LDAP group can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign an LDAP group to hierarchical roles directly.

Memberships – LDAP group (page description)

To open the **Memberships – LDAP group** page go to **Responsibilities** > **Auditing** > **LDAP** > **Show details** > **Memberships**.

On the **Memberships - LDAP group** page, you can see identities to which the LDAP group is assigned (see Displaying memberships in system entitlements on page 578).

The following table gives an overview of the different content on the **Memberships – LDAP group** page.

Table 746: Columns

Column	Description
Identity	Shows you the name of the identity to which the LDAP group is assigned.
Origin	Shows whether the LDAP group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – LDAP group (page description)

To open the **Attestation – LDAP group** page go to **Responsibilities** > **Auditing** > **LDAP** > **Show details** > **Attestation**.

On the **Attestation - LDAP group** page, you can:

- Display all attestation cases linked to this LDAP group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve LDAP group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the various features and content on the **Attestation - LDAP group** page.

Table 747: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 748: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 749: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Child groups – LDAP group (page description)

To open the **Compliance - LDAP group** page go to **Responsibilities** > **Auditing** > **LDAP** > **Show details** > **Compliance**.

On the **Compliance - LDAP group** page, you can see all the child groups of the LDAP group (see Displaying system entitlement child groups on page 578).

History – LDAP group (page description)

To open the **History – LDAP group** page go to **Responsibilities** > **Auditing** > **LDAP** > **Show details** > **History**.

On the **History – LDAP group** page, you can see all the changes made to the LDAP group (see System entitlement history on page 581).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.
- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – LDAP** page.

Table 750: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 751: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 752: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – LDAP group (page description)

To open the **Usage – LDAP group** page go to **Responsibilities** > **Auditing** > **LDAP** > **Show details** > **Usage**.

On the **Usage – LDAP group** page, you can see the roles and organizations that belong to the identities to which the LDAP group is assigned (see Displaying role memberships of system entitlement members on page 584).

The following tables give you an overview of the different functions on the **Usage - LDAP** page.

Table 753: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Oracle E-Business Suite (page description)

To open the **Auditing - Oracle E-Business Suite** page go to **Responsibilities** > **Auditing** > **Oracle E-Business Suite**.

On the **Auditing - Oracle E-Business Suite** page, you can see all the E-Business Suite groups (see Displaying all system entitlements on page 576).

If you click **Show details** in an E-Business Suite group's details pane, a new page opens (see Auditing – Oracle E-Business Suite (page description) on page 1332) that contains more information and configuration options for the E-Business Suite group.

The following tables give you an overview of the various features and content on the **Auditing - Oracle E-Business Suite** page.

Table 754: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the E-Business Suite groups they manage are shown (see Displaying all system entitlements on page 576).

Table 755: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: E-Business Suite**

Control	Description
	group page (see Auditing – E-Business Suite group (page description) on page 1333). Use this button to display more details about the E-Business Suite group.

Table 756: Columns

Column	Description
Display	Shows the E-Business Suite group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing – E-Business Suite group (page description)

To open the **Auditing - Roles and entitlements: E-Business Suite group** page go to **Responsibilities** > **Auditing** > **Oracle E-Business Suite** > **Show details**.

On the **Auditing - Roles and entitlements: E-Business Suite group** page, you can access various information about the selected E-Business Suite group.

To do this, click on one of the tiles:

Table 757: Tiles

Tile	Description
Overview	Opens the **Overview – Overview – E-Business Suite group (page description) on page 1334 group** page (see E-Business Suite). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – E-Business Suite group** (see Main data – E-Business Suite group (page description) on page 1334). Here you can see the E-Business Suite group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – E-Business Suite group** page (see Memberships – E-Business Suite group (page description) on page 1335). Here you can see identities to which the E-Business Suite group is assigned (see Displaying memberships in system entitlements on page 578).
Attestation	Opens the **Attestation – E-Business Suite group** (see Attestations –

Tile	Description
	E-Business Suite group (page description) on page 1336). You select the following actions: • Display all attestation cases linked to this E-Business Suite group (see Displaying attestation cases of system entitlements on page 579) • Display identities that have yet to approve E-Business Suite group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)
History	Opens the **History – E-Business Suite group** page (see History – E-Business Suite group (page description) on page 1338). Here you can see all the changes made to the E-Business Suite group (see System entitlement history on page 581).
Usage	Opens the **Usage – E-Business Suite group** page (see Usage – E-Business Suite group (page description) on page 1340). Here you can see which roles the members of the E-Business Suite group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – E-Business Suite group (page description)

To open the **Overview - E-Business Suite group** page go to **Responsibilities** > **Auditing** > **Oracle E-Business Suite** > **Show details** > **Overview**.

On the **Overview – E-Business Suite group** page, you can see all the information relevant to the E-Business Suite group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – E-Business Suite group (page description)

To open the **Main data – E-Business Suite group** page go to **Responsibilities** > **Auditing** > **Oracle E-Business Suite** > **Show details** > **Main data**.

On the **Main data – E-Business Suite group** page, you can see the E-Business Suite group's main data (see Displaying system entitlement main data on page 577).

Enter the following main data:

Table 758: E-Business Suite group main data

Property	Description
Name	Shows you the full, descriptive name of the E-Business Suite group.
Canonical name	Shows you the automatically generated canonical name of the E-Business Suite group.
Distinguished name	Shows you the automatically generated distinguished name of the E-Business Suite group.
Display name	Shows you the name of the E-Business Suite group used to display E-Business Suite group in the One Identity Manager tools.
Container	Shows you the parent container of the E-Business Suite group.
Service item	Shows you the assigned service items.
Category	Shows you the category for E-Business Suite group inheritance. User accounts can inherit E-Business Suite groups selectively. To do this, E-Business Suite groups and user accounts are divided into categories.
Description	Shows you the E-Business Suite group's description.
Risk index	Shows you the configured risk index. This value specifies the risk of assigning this E-Business Suite group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the E-Business Suite group can be requested in the IT Shop. If set, the E-Business Suite group can be requested by identities using the Web Portal and granted through a defined approval process. The E-Business Suite group can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows you whether the E-Business Suite group can only be requested through the IT Shop. If set, the E-Business Suite group can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign an E-Business Suite group to hierarchical roles directly.

Memberships – E-Business Suite group (page description)

To open the **Memberships – E-Business Suite group** page go to **Responsibilities** > **Auditing** > **Oracle E-Business Suite** > **Show details** > **Memberships**.

On the **Memberships - E-Business Suite group** page, you can see identities to which the E-Business Suite group is assigned (see Displaying memberships in system entitlements on page 578).

The following table gives an overview of the different content on the **Memberships – E-Business Suite group** page.

Table 759: Columns

Column	Description
Identity	Shows you the name of the identity to which the E-Business Suite group is assigned.
Origin	Shows whether the E-Business Suite group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – E-Business Suite group (page description)

To open the **Attestation – E-Business Suite group** page go to **Responsibilities** > **Auditing** > **Oracle E-Business Suite** > **Show details** > **Attestation**.

On the **Attestation – E-Business Suite group** page, you can:

- Display all attestation cases linked to this E-Business Suite group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve E-Business Suite group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the various features and content on the **Attestation - E-Business Suite group** page.

Table 760: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 761: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 762: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

History – E-Business Suite group (page description)

To open the **History – E-Business Suite group** page go to **Responsibilities** > **Auditing** > **Oracle E-Business Suite** > **Show details** > **History**.

On the **History – E-Business Suite group** page, you can see all the changes made to the E-Business Suite group (see System entitlement history on page 581).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Oracle E-Business Suite** page.

Table 763: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 764: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 765: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – E-Business Suite group (page description)

To open the **Usage – E-Business Suite group** page go to **Responsibilities** > **Auditing** > **Oracle E-Business Suite** > **Show details** > **Usage**.

On the **Usage – E-Business Suite group** page, you can see the roles and organizations that belong to the identities to which the E-Business Suite group is assigned (see Displaying role memberships of system entitlement members on page 584).

The following tables give you an overview of the different functions on the **Usage - Oracle E-Business Suite** page.

Table 766: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Privileged Account Management (page description)

To open the **Auditing - Privileged Account Management** page go to **Responsibilities** > **Auditing** > **Privileged Account Management**.

On the **Auditing - Privileged Account Management** page, you can see all the PAM groups (see Displaying all system entitlements on page 576).

If you click **Show details** in a PAM group's details pane, a new page opens (see Auditing - Roles and permissions: PAM group (page description) on page 1341) that contains more information and configuration options for the PAM group.

The following tables give you an overview of the various features and content on the **Auditing - Privileged Account Management** page.

Table 767: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the PAM groups they manage are shown (see Displaying all system entitlements on page 576).

Table 768: Columns

Column	Description
Display	Shows the PAM group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: PAM group (page description)

To open the **Auditing - Roles and entitlements: PAM group** page go to **Responsibilities** > **Auditing** > **Privileged Account Management** > **Show details**.

On the **Auditing - Roles and entitlements: PAM group** page, you can access various information about the selected PAM group.

To do this, click on one of the tiles:

Table 769: Tiles

Tile	Description
Overview	Opens the **Overview – Overview – PAM group (page description) on page 1342 group** page (see PAM). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – PAM group** (see Main data – PAM group (page description) on page 1342). Here you can see and edit the PAM group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – PAM group** page (see Memberships – PAM group (page description) on page 1343). Here you can see identities to which the PAM group is assigned (see Displaying memberships in system entitlements on page 578).
Attestation	Opens the **Attestation – PAM group** (see Attestations – PAM group (page description) on page 1344). You select the following actions: • Display all attestation cases linked to this PAM group (see Displaying attestation cases of system entitlements on page 579) • Display identities that have yet to approve PAM group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)
History	Opens the **History – PAM group** page (see History – PAM group (page description) on page 1345).

Tile	Description
	Here you can see all the changes made to the PAM group (see System entitlement history on page 581).
Usage	Opens the **Usage – PAM group** page (see Usage – PAM group (page description) on page 1347). Here you can see which roles the members of the PAM group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – PAM group (page description)

To open the **Overview - PAM group** page go to **Responsibilities** > **Auditing** > **Privileged Account Management** > **Show details** > **Overview**.

On the **Overview – PAM group** page, you can see all the information relevant to the PAM group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – PAM group (page description)

To open the **Main data – PAM group** page go to **Responsibilities** > **Auditing** > **Privileged Account Management** > **Show details** > **Main data**.

On the **Main data – PAM group** page, you can see the PAM group's main data (see Displaying system entitlement main data on page 577).

Enter the following main data:

Table 770: PAM group main data

Property	Description
Name	Shows you the full, descriptive name of the PAM group.
Canonical name	Shows you the automatically generated canonical name of the PAM group.
Distinguished name	Shows you the automatically generated distinguished name of the PAM group.
Display name	Shows you the name of the PAM group used to display PAM group in the One Identity Manager tools.
Container	Shows you the parent container of the PAM group.
Service item	Shows you the assigned service items.
Category	Shows you the category for PAM group inheritance.

Property	Description
	User accounts can inherit PAM groups selectively. To do this, PAM groups and user accounts are divided into categories.
Description	Shows you the PAM group's description.
Risk index	Shows you the configured risk index. This value specifies the risk of assigning this PAM group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the PAM group can be requested in the IT Shop. If set, the PAM group can be requested by identities using the Web Portal and granted through a defined approval process. The PAM group can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows you whether the PAM group can only be requested through the IT Shop. If set, the PAM group can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign a PAM group to hierarchical roles directly.

Memberships – PAM group (page description)

To open the **Memberships – PAM group** page go to **Responsibilities** > **Auditing** > **Privileged Account Management** > **Show details** > **Memberships**.

On the **Memberships - PAM group** page, you can see identities to which the PAM group is assigned (see Displaying memberships in system entitlements on page 578).

The following table gives an overview of the different content on the **Memberships – PAM group** page.

Table 771: Columns

Column	Description
Identity	Shows you the name of the identity to which the PAM group is assigned.
Origin	Shows whether the PAM group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – PAM group (page description)

To open the **Attestation – PAM group** page go to **Responsibilities** > **Auditing** > **Privileged Account Management** > **Show details** > **Attestation**.

On the **Attestation – PAM group** page, you can:

- Display all attestation cases linked to this PAM group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve PAM group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the various features and content on the **Attestation - PAM group** page.

Table 772: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 773: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 774: Columns

Column	Description
Display	Shows the name of the object included in the attestation case.

Column	Description
name	
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

History – PAM group (page description)

To open the **History – PAM group** page go to **Responsibilities** > **Auditing** > **Privileged Account Management** > **Show details** > **History**.

On the **History – PAM group** page, you can see all the changes made to the PAM group (see System entitlement history on page 581).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Privileged Account Management** page.

Table 775: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 776: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 777: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.

Column	Description
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – PAM group (page description)

To open the **Usage – PAM group** page go to **Responsibilities** > **Auditing** > **Privileged Account Management** > **Show details** > **Usage**.

On the **Usage – PAM group** page, you can see the roles and organizations that belong to the identities to which the PAM group is assigned (see Displaying role memberships of system entitlement members on page 584).

The following tables give you an overview of the different functions on the **Usage - Privileged Account Management** page.

Table 778: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – SAP R/3 (page description)

To open the **Auditing - SAP R/3** page go to **Responsibilities** > **Auditing** > **SAP R/3**.

On the **Auditing - SAP R/3** page, you can see all the SAP groups (see Displaying all system entitlements on page 576).

If you click **Show details** in an SAP group's details pane, a new page opens (see Auditing - Roles and permissions: SAP group (page description) on page 1349) that contains more information and configuration options for the SAP group.

The following tables give you an overview of the various features and content on the **Auditing - SAP R/3** page.

Table 779: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the SAP groups they manage are shown (see Displaying all system entitlements on page 576).

Table 780: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: SAP group** page (see Auditing - Roles and permissions: SAP group (page description) on page 1349). Use this button to display more details about the SAP group.

Table 781: Columns

Column	Description
Display	Shows the SAP group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: SAP group (page description)

To open the **Auditing - Roles and entitlements: SAP group** page go to **Responsibilities** > **Auditing** > **SAP R/3** > **Show details**.

On the **Auditing - Roles and entitlements: SAP group** page, you can access various information about the selected SAP group.

To do this, click on one of the tiles:

Table 782: Tiles

Tile	Description
Overview	Opens the **Overview – Overview – SAP group (page description) on page 1350 group** page (see SAP). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – SAP group** (see Main data – SAP group (page description) on page 1350). Here you can see the SAP group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – SAP group** page (see Memberships – SAP group (page description) on page 1351). Here you can see identities to which the SAP group is assigned (see Displaying memberships in system entitlements on page 578).
Attestation	Opens the **Attestation – SAP group** (see Attestations – SAP group (page description) on page 1352). You select the following actions: • Display all attestation cases linked to this SAP group (see Displaying attestation cases of system entitlements on page 579) • Display identities that have yet to approve SAP group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)
History	Opens the **History – SAP group** page (see History – SAP group (page description) on page 1353). Here you can see all the changes made to the SAP group (see System entitlement history on page 581).
Usage	Opens the **Usage – SAP group** page (see Usage – SAP group (page

Tile	Description
	description) on page 1355). Here you can see which roles the members of the SAP group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – SAP group (page description)

To open the **Overview - SAP group** page go to **Responsibilities** > **Auditing** > **SAP R/3** > **Show details** > **Overview**.

On the **Overview – SAP group** page, you can see all the information relevant to the SAP group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – SAP group (page description)

To open the **Main data – SAP group** page go to **Responsibilities** > **Auditing** > **SAP R/3** > **Show details** > **Main data**.

On the **Main data – SAP group** page, you can see the SAP group's main data (see Displaying system entitlement main data on page 577).

Enter the following main data:

Table 783: SAP group main data

Property	Description
Name	Shows you the full, descriptive name of the SAP group.
Canonical name	Shows you the automatically generated canonical name of the SAP group.
Distinguished name	Shows you the automatically generated distinguished name of the SAP group.
Display name	Shows you the name of the SAP group used to display SAP group in the One Identity Manager tools.
Container	Shows you the parent container of the SAP group.
Service item	Shows you the assigned service items.
Category	Shows you the category for SAP group inheritance. User accounts can inherit SAP groups selectively. To do this, SAP groups and user accounts are divided into categories.
Description	Shows you the SAP group's description.

Property	Description
Risk index	Shows you the configured risk index. This value specifies the risk of assigning this SAP group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the SAP group can be requested in the IT Shop. If set, the SAP group can be requested by identities using the Web Portal and granted through a defined approval process. The SAP group can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Shows you whether the SAP group can only be requested through the IT Shop. If set, the SAP group can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign an SAP group to hierarchical roles directly.

Memberships – SAP group (page description)

To open the **Memberships – SAP group** page go to **Responsibilities** > **Auditing** > **SAP R/3** > **Show details** > **Memberships**.

On the **Memberships - SAP group** page, you can see identities to which the SAP group is assigned (see Displaying memberships in system entitlements on page 578).

The following table gives an overview of the different content on the **Memberships – SAP group** page.

Table 784: Columns

Column	Description
Identity	Shows you the name of the identity to which the SAP group is assigned.
Origin	Shows whether the SAP group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – SAP group (page description)

To open the **Attestation – SAP group** page go to **Responsibilities** > **Auditing** > **SAP R/3** > **Show details** > **Attestation**.

On the **Attestation – SAP group** page, you can:

- Display all attestation cases linked to this SAP group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve SAP group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the various features and content on the **Attestation - SAP group** page.

Table 785: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 786: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 787: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case.

Column	Description
	The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

History – SAP group (page description)

To open the **History – SAP group** page go to **Responsibilities** > **Auditing** > **SAP R/3** > **Show details** > **History**.

On the **History – SAP group** page, you can see all the changes made to the SAP group (see System entitlement history on page 581).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – SAP R/3** page.

Table 788: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 789: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 790: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.

Column	Description
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – SAP group (page description)

To open the **Usage – SAP group** page go to **Responsibilities** > **Auditing** > **SAP R/3** > **Show details** > **Usage**.

On the **Usage – SAP group** page, you can see the roles and organizations that belong to the identities to which the SAP group is assigned.

The following tables give you an overview of the different functions on the **Usage - SAP R/3** page.

Table 791: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Auditing – Unix (page description)

To open the **Auditing - Unix** page go to **Responsibilities** > **Auditing** > **Unix**.

On the **Auditing - Unix** page, you can see all the Unix groups (see Displaying all system entitlements on page 576).

If you click **Show details** in a Unix group's details pane, a new page opens (see Auditing - Roles and permissions: Unix group (page description) on page 1356) that contains more information and configuration options for the Unix group.

The following tables give you an overview of the various features and content on the **Auditing - Unix** page.

Table 792: Controls

Control	Description
Select an identity	Use this feature to select an identity so that only the Unix groups they manage are shown (see Displaying all system entitlements on page 576).

Table 793: Controls in the details pane of a product

Control	Description
Show details	Opens the **Auditing - roles and entitlements: Unix group** page (see Auditing - Roles and permissions: Unix group (page description) on page 1356). Use this button to display more details about the Unix group.

Table 794: Columns

Column	Description
Display	Shows the Unix group's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Auditing - Roles and permissions: Unix group (page description)

To open the **Auditing - Roles and entitlements: Unix group** page go to **Responsibilities** > **Auditing** > **Unix** > **Show details**.

On the **Auditing - Roles and entitlements: Unix group** page, you can access various information about the selected Unix group.

To do this, click on one of the tiles:

Table 795: Tiles

Tile	Description
Overview	Opens the **Overview – Overview – Unix group (page description) on page 1357 group** page (see Unix). This provides you with all the information at a glance. For more information, click on the links inside one of the shapes (see Displaying system entitlement overviews on page 577).
Main data	Opens the **Main data – Unix group** (see Main data – Unix group (page description) on page 1358). Here you can see the Unix group's main data (see Displaying system entitlement main data on page 577).
Memberships	Opens the **Memberships – Unix group** page (see Memberships – UNIX group (page description) on page 1359). Here you can see identities to which the Unix group is assigned (see Displaying memberships in system entitlements on page 578).
Attestation	Opens the **Attestation – Unix group** (see Attestations – Unix group (page description) on page 1359). You select the following actions: • Display all attestation cases linked to this Unix group (see Displaying attestation cases of system entitlements on page 579) • Display identities that have yet to approve Unix group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580) • Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)
History	Opens the **History – Unix group** page (see History – Unix group (page description) on page 1361). Here you can see all the changes made to the Unix group (see System entitlement history on page 581).
Usage	Opens the **Usage – Unix group** page (see Usage – Unix group (page description) on page 1363). Here you can see which roles the members of the Unix group belong to (see Displaying role memberships of system entitlement members on page 584).

Overview – Unix group (page description)

To open the **Overview - Unix group** page go to **Responsibilities** > **Auditing** > **Unix** > **Show details** > **Overview**.

On the **Overview – Unix group** page, you can see all the information relevant to the Unix group summarized in an overview (see Displaying system entitlement overviews on page 577).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Unix group (page description)

To open the **Main data – Unix group** page go to **Responsibilities** > **Auditing** > **Unix** > **Show details** > **Main data**.

On the **Main data – Unix group** page, you can see the Unix group's main data (see Displaying system entitlement main data on page 577).

Enter the following main data:

Table 796: Unix group main data

Property	Description
Name	Shows you the full, descriptive name of the Unix group.
Canonical name	Shows you the automatically generated canonical name of the Unix group.
Distinguished name	Shows you the automatically generated distinguished name of the Unix group.
Display name	Shows you the name of the Unix group used to display Unix group in the One Identity Manager tools.
Container	Shows you the parent container of the Unix group.
Service item	Shows you the assigned service items.
Category	Shows you the category for Unix group inheritance. User accounts can inherit Unix groups selectively. To do this, Unix groups and user accounts are divided into categories.
Description	Shows you the Unix group's description.
Risk index	Shows you the configured risk index. This value specifies the risk of assigning this Unix group to a user account. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Shows you whether the Unix group can be requested in the IT Shop. If set, the Unix group can be requested by identities using the Web Portal and granted through a defined approval process. The Unix group can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the *One Identity Manager IT*

Property	Description
	Shop Administration Guide.
Only use in IT Shop	Shows you whether the Unix group can only be requested through the IT Shop. If set, the Unix group can be requested by identities using the Web Portal and granted through a defined approval process. You cannot assign a Unix group to hierarchical roles directly.

Memberships – UNIX group (page description)

To open the **Memberships – Unix group** page go to **Responsibilities** > **Auditing** > **Unix** > **Show details** > **Memberships**.

On the **Memberships - Unix group** page, you can see identities to which the Unix group is assigned (see Displaying memberships in system entitlements on page 578).

The following table gives an overview of the different content on the **Memberships – Unix group** page.

Table 797: Columns

Column	Description
Identity	Shows you the name of the identity to which the Unix group is assigned.
Origin	Shows whether the Unix group is assigned directly or indirectly to the employee.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity obtained the membership through a request, you will find more information on the following tabs on the **Request** tab:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestations – Unix group (page description)

To open the **Attestation – Unix group** page go to **Responsibilities** > **Auditing** > **Unix** > **Show details** > **Attestation**.

On the **Attestation - Unix group** page, you can:

- Display all attestation cases linked to this Unix group (see Displaying attestation cases of system entitlements on page 579)
- Display identities that have yet to approve Unix group attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 580)
- Display details of the objects being attested (see Displaying attestation cases of system entitlements on page 579)

The following tables give you an overview of the various features and content on the **Attestation - Unix** page.

Table 798: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases and Then you can send reminder emails to these identities (see Displaying attestors of system entitlement pending attestation cases on page 580).

Table 799: Controls in the attestation case's details pane

Control	Description
Show details	Use this button to display all the objects involved in the attestation case (see Displaying attestation cases of system entitlements on page 579).

Table 800: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been

Column	Description
	granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

History – Unix group (page description)

To open the **History – Unix group** page go to **Responsibilities** > **Auditing** > **Unix** > **Show details** > **History**.

On the **History – Unix group** page, you can see all the changes made to the Unix group (see System entitlement history on page 581).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Unix** page.

Table 801: Controls

Control	Description
Events	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user (see Displaying system entitlement history on page 582). TIP: To remove the filter again, click **Reset filter** next to the corresponding filter.

Control	Description
Switch to table view	Use this button to display the changes in table form (see Displaying system entitlement history on page 582).
Switch to timeline view	Use this button to display the changes as a timeline.(see Displaying system entitlement history on page 582).
Status comparison	
Time and date picker	Select from which point on you want to see the changes (see Comparing statuses of system entitlements on page 583).
Display changed values only	Deselect the check box if you also want to display properties that have not changed since they were created (see Comparing statuses of system entitlements on page 583).

Table 802: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 803: Columns

Column	Description
Events (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.

Column	Description
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Unix group (page description)

To open the **Usage – Unix group** page go to **Responsibilities** > **Auditing** > **Unix** > **Show details** > **Usage**.

On the **Usage – Unix group** page, you can see the roles and organizations that belong to the identities to which the Unix group is assigned.

The following tables give you an overview of the different functions on the **Usage - Unix** page.

Table 804: Controls

Control	Description
Role classes	Use this list of roles and organizations to select what you want to view.
More information	Use this button to show the legend that explains the content of the overview.

Governance administration (page description)

To open the **Governance Administration** page go to **Responsibilities** > **Governance Administration**.

On the **Governance Administration** page, you can manage all objects.

To do this, click on one of the tiles:

- Organization (includes departments, cost centers, and locations)
- Identities
- Business roles
- System entitlements
- Resources
- Multi-request resources
- Multi requestable/unsubscribable resources
- Assignment resources
- System roles

Business roles (page description)

To open the **Business Roles** page go to **Responsibilities** > **Governance Administration** > **Business Roles**.

On the **Business Roles** page, you can:

- Display all business roles (see Displaying all business roles on page 617)
- Restore deleted business roles (see Restoring deleted business roles on page 617)

If you click **Edit** in a business role's details pane, a new page opens, which contains more information and configuration options for the business role (see Business role (page description) on page 1365).

The following tables give you an overview of the various features and content on the **Business roles** page.

Table 805: Controls

Control	Description
To restore a deleted role	Use this button to restore a deleted business role (see Restoring deleted business roles on page 617).

Table 806: Columns

Column	Description
Display	Shows you the business role's name.
Manager	Shows you which identity is responsible for the business role.
Role class	Shows you which role class the business role belongs to.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Business role (page description)

To open the **Business role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit**.

On the **Business role** page, you can perform various actions on the business role you selected beforehand.

To do this, click on one of the tiles:

Table 807: Tiles

Tiles	Description
Overview	Opens the **Overview - Business role** page (see Overview – Business role (page description) on page 1367). This provides you with all the information at a glance (see Displaying business role overviews on page 619). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Business role** page (see Main data – Business role (page description) on page 1367). Here you can view and edit the business role's main data (see Displaying and editing business role main data on page 619).
Memberships	Opens the **Memberships - Business role** page (see Memberships – Business role (page description) on page 1368). You select the following actions: • Display identities that are assigned this business role (see Displaying business role memberships on page 620) • Request the business role for identities (see Assigning identities to business roles on page 621) • Cancel this business role for identities (see Removing business roles from identities on page 621)
Permissions	Opens the **Entitlements – Business role** page (see Entitlements – Business role (page description) on page 1370). You select the following actions: • Display entitlements assigned to the business role (see Displaying business role entitlements on page 622) • Add new entitlements (see Adding business role entitlements on page 623) • Delete business role entitlements (see Deleting business role entitlements on page 624)
Compliance	Opens the **Compliance – Business role** page (see Compliance – Business role (page description) on page 1371).

Tiles	Description
	Here you see compliance rule violations that were caused by this business role (see Displaying business role rule violations on page 625).
Attestation	Opens the **Attestation – Business role** page (see Attestation – Business role (page description) on page 1371). You select the following actions: • Display all attestation cases linked to this business role (see Displaying business role attestation cases on page 628) • Display details of the objects being attested (see Displaying business role attestation cases on page 628) • Make approval decisions about pending attestation cases (see Approving and denying business role attestation cases on page 630) • Display attestors of pending attestation cases (see Displaying attestors of business role pending attestation cases on page 629) • Send reminders to approvers (see Sending reminders about business role pending attestation cases on page 631)
Risk	Opens the **Risk – Business role** page (see Risk – Business role (page description) on page 1373). You select the following actions: • Display the business role's calculated risk index (see Displaying business role risk indexes on page 633) • Show how the calculated risk index is put together
History	Opens the **History – Business role** page (see History – Business role (page description) on page 1374). Here you can view all changes made to the business role (see Business role history on page 634).
Usage	Opens the **Usage – Business role** page (see Usage – Business role (page description) on page 1376). Here you can display which roles the members of the business role belong to (see Displaying role memberships of business role members on page 637).
Compliance reports	Opens the **Compliance report – Business role** page (see Compliance reports – Business role (page description) on page 1376). You select the following actions: • Display the business role's policy violations (see Displaying business role policy violations on page 626)

Tiles	Description
	• Display rule violations of business role members (see Displaying rule violations of business role members on page 626) • Display risk indexes and entitlements of business role members (see Displaying risk indexes and entitlements of business role members on page 627)
Split	Here you can split the business role into two (see Copying/splitting business roles on page 638).
Compare and merge	Here you can compare and merge the business role with another role (business role, department, cost center or location) (see Comparing and merging business roles on page 639).
Redo	Here you can restore a deleted business role that was under this business role (see Restoring deleted business roles on page 617).

Overview – Business role (page description)

To open the **Overview - Business Role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit> Overview**.

On the **Overview - Business role** page, you can display all relevant information about the business role summarized in an overview (see Displaying business role overviews on page 619).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Business role (page description)

To open the **Main data - Business Role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit> Main data**

On the **Main data - Business role** page, you can show and edit the business role's main data (see Displaying and editing business role main data on page 619).

The following tables give you an overview of the different functions and content on the **Main data – Business role** page.

Table 808: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 809: Business role main data

Property	Description
Business role	Enter a full, descriptive name for the business role.
Short name	Enter a short name for the business role.
Internal name	Enter a company internal name for the business role.
Description	Enter a description for the business role.
Role class	When you create the business role: Select the role class of the business role. To differentiate between different business roles, define company specific role classes. Role classes are used to specify which company resource assignments are possible through roles in a role class.
Parent business role	Click **Assign**/**Change** and select a business role to be the parent business role for organizing the business role hierarchically. If you want the business role at the root of a business role hierarchy, leave the field empty.
Role type	Select the role type of the business role. Role types are mainly used to regulate approval policy inheritance.
Role approver	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the business role.
Role approver (IT)	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the business role.
Manager	Click **Assign**/**Change** and select the manager responsible for the business role.
2nd Manager	Click **Assign**/**Change** and select an identity to act as a deputy to the business role's manager.
Employees do not inherit	Select this check box if you want to temporarily prevent identities from inheriting this business role.
Comment	Enter a comment for the business role.

Memberships – Business role (page description)

To open the **Memberships – Business Role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit** > **Memberships**.

On the **Memberships – Business role** page, you can:

- Display identities that are assigned this business role (see Displaying business role memberships on page 620)
- Request the business role for identities (see Assigning identities to business roles on page 621)
- Cancel this business role for identities (see Removing business roles from identities on page 621)

The following tables give you an overview of the different functions and content on the **Memberships – Business role** page.

Table 810: Controls

Control	Description
Request memberships	Use this button to request the business role for identities (see Assigning identities to business roles on page 621).
Delete member-ships	Use this button to delete membership of selected identities in the business role (see Removing business roles from identities on page 621). Select the check box in front of the identities whose membership in the business role you want to delete and click this button.

Table 811: Columns

Column	Description
Identity	Shows you the name of the identity to which the business role is assigned.
Origin	Shows you whether the business role was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Business role (page description)

To open the **Entitlements - Business Role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit** > **Entitlements**.

On the **Entitlements – Business role** page, you can:

- Display entitlements assigned to the business role (see Displaying business role entitlements on page 622)
- Add new entitlements (see Adding business role entitlements on page 623)
- Delete business role entitlements (see Deleting business role entitlements on page 624)

TIP: Entitlements form the basis for membership in an object (for example in a department).

The following tables give you an overview of the various features and content on the **Entitlements – Business role** page.

Table 812: Controls

Control	Description
New	Use this button to add a new entitlement to the business role (see Adding business role entitlements on page 623). Identities that this business role is assigned to, automatically obtain membership in the object assigned here.
Remove	You can use this button to delete selected permissions (see Deleting business role entitlements on page 624)(see Deleting department entitlements on page 598)(see Deleting cost center entitlements on page 667)(see Deleting entitlements from locations on page 723). To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 813: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Business role (page description)

To open the **Compliance - Business Role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit** > **Compliance**.

On the **Compliance - Business Role** page, you can view compliance rule violations caused by the business role (see Displaying business role rule violations on page 625).

The following table gives an overview of the content of the **Compliance – Business role** page.

Table 814: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Business role (page description)

To open the **Attestation - Business Role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit** > **Attestation**.

On the **Attestation - Business Role** page you can:

- Display all attestation cases linked to this business role (see Displaying business role attestation cases on page 628)
- Display details of the objects being attested (see Displaying business role attestation cases on page 628)
- Make approval decisions about pending attestation cases (see Approving and denying business role attestation cases on page 630)

- Display attestors of pending attestation cases (see Displaying attestors of business role pending attestation cases on page 629)
- Send reminders to approvers (see Sending reminders about business role pending attestation cases on page 631)

The following tables give you overview of the various features and contents of the **Attestation – Business Role** page.

Table 815: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of business role pending attestation cases on page 629) Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about business role pending attestation cases on page 631).
Approve	Opens the **Pending Attestations – Business roles** (see Pending attestations – Business role (page description) on page 920). Use this button to make approval decisions about attestation cases pending for the business role (see Approving and denying business role attestation cases on page 630).

Table 816: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of business role pending attestation cases on page 629) Then you can send reminder emails to these identities (see Sending reminders about business role pending attestation cases on page 631).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying business role attestation cases on page 628)

Table 817: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.

Column	Description
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Business role (page description)

To open the **Risk – Business role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit** > **Risk**.

On the **Risk – Business role** page, you can:

- Display the business role's calculated risk index (see Displaying business role risk indexes on page 633)
- Show how the calculated risk index is put together

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the various features and content on the **Risk – Business role** page.

Table 818: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index.

Table 819: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Business role (page description)

To open the **History - Business Role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit** > **History**.

On the **History – Business Role** page you can see all changes made to the business role (see Business role history on page 634).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows you all the events that affect a business role, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Business role** page.

Table 820: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user.

Control	Description
	TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Disable this check box if you also want to see properties that have not changed since they were created.

Table 821: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 822: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.

Column	Description
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Business role (page description)

To open the **Usage - Business role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit** > **Usage**.

On the **Usage - Business role** page, you can see which roles the business role members belong to (see Displaying role memberships of business role members on page 637).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the different functions on the **Usage – Business role** page.

Table 823: Controls

Control	Description
Role classes	You can select the main category of roles and organizations you want to display from this menu.
More information	Use this button to show the legend that explains the content of the overview.

Compliance reports – Business role (page description)

To open the **Compliance Reports – Business Role** page go to **Responsibilities** > **Governance Administration** > **Business Roles** > **Edit** > **Compliance Reports**.

On the **Compliance Reports – Business role** page you can:

- Display the business role's policy violations (see Displaying business role policy violations on page 626)
- Display rule violations of business role members (see Displaying rule violations of business role members on page 626)
- Display risk indexes and entitlements of business role members (see Displaying risk indexes and entitlements of business role members on page 627)

The information is divided into three parts:

- **Policy violations**: Shows all the current policy violations caused by the application role.
- **Compliance rule violations**: Shows you the current rule violations of the identities to which the business role is assigned.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and entitlements**: Displays all identities to which the business role is assigned. In addition, the number of entitlements and risk index assigned to these identities is displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – Business role** page.

Table 824: Columns

Column	Description
Policy violations	
Violating object	Show which object caused the rule violation.
Policy	Show the policy that was violated.
Status	Show the status of the rule policy.
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows the violated rule.
Approval state	Shows how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

Column	Description
Identities: Risk index and entitlements	
Identity	Shows you the identity to which this business role is assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Identities (page description)

To open the **Identities** page go to **Responsibilities** > **Governance Administration** > **Identities**.

On the **Identities** page, you can:

- Display all identities (see Displaying all identities on page 641)
- Add new identities (see Adding identities on page 642)

If you click an identity in the list, a new page opens, which contains more information and configuration options for the identity (see Identity (page description) on page 1380).

The following tables give you an overview of the various features and content on the **Identities** page.

Table 825: Controls

Control	Description
Add a new identity	Opens the **Add a New Identity** page (see Adding a new identity (page description) on page 1379). Use this button to add a new identity to the system (see Adding identities on page 642).

Table 826: Columns

Column	Description
Display	Shows you the identity's name.
Primary department	Shows the department that the identity is primarily assigned to.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Adding a new identity (page description)

To open the **Add a New Identity** page go to **Responsibilities** > **Governance Administration** > **Identities** > **Add a new identity**.

On the **Add a New Identity** page, you can add a new identity by providing its main data (see Adding your own identities on page 301).

Enter the following main data.

Table 827: Identities main data

Property	Description
Personal data	
Last name	Enter the identity's last name.
First name	Enter the identity's first name.
Middle name	Enter the identity's middle name.
Date of birth	Enter the identity's date of birth. Click the (**Calendar**) to do this and use the date picker to select the date of birth.
Personnel number	Enter the identity's personnel number.
Gender	In the menu, select the identity's gender.
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Organizational information	
Primary cost center	Click **Assign**/**Change** and select the identity's primary cost center.
Primary department	Click **Assign**/**Change** and select the identity's primary department.
External	Select the check box if this is an external identity.
Employee type	In the menu, select what type of identity this is. For example, an identity of this company or a trainee.
Entry date	Enter the date the identity started at the company. Click the (**Calendar**) and use the date picker to select the starting date.
Leaving date	Enter the date that the identity leaves the company. Click the (**Calendar**) to do this and use the date picker to select the leaving date.
Manager	Shows you the identity's manager.

Property	Description
	TIP: If necessary, you can transfer the identity's manager at a later date (see Assigning other managers to my identities on page 299).
Primary location	Click **Assign**/**Change** and select the identity's primary location.
Building	Enter the building where the identity works.
Floor	Enter which floor the identity works on.
Room	Enter the room the identity works in.
Street	Enter the road where the identity works.
Zip code	Enter the zip code of the identity's work location.
City	Enter the city where the identity works.

Identity (page description)

To open the **Identity** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity.

On the **Identity** page, you can perform various actions on the identity you selected beforehand.

To do this, click on one of the tiles:

Table 828: Tiles

Tiles	Description
Overview	Opens the **Overview - Identity** page (see Overview – Identity (page description) on page 1382). This provides you with all the information at a glance (see Displaying identity overviews on page 643). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data – Identity** page (see Main data – Identity (page description) on page 1382). You perform the following actions: • Displaying and editing the identity's main data (see Displaying and editing identity main data on page 643) • Transfer responsibility of the identity to another manager (see Assigning other managers to identities on page 644) • Create reports on identity data (see Creating reports about identities on page 645)

Tiles	Description
My Requests	Opens the **Requests – Identity** page (see Requests - Identities ((page description)) on page 1385). Here you can see all the products that this identity has requested or were requested for them (see Displaying identity requests on page 645).
Permissions	Opens the **Entitlements – Identity** page (see Entitlements – Identity (page description) on page 1387). You select the following actions: • Display entitlements assigned to the identity (see Displaying identity entitlements on page 646) • Remove the identity's entitlements (see Deleting identity entitlements on page 647)
Delegations	Opens the **Delegations – Identity** page (see Delegations – Identity (page description) on page 1388). You select the following actions: • Display all delegations that the identity is involved in (see Displaying identity delegations on page 648) • Delegate the identity's role memberships and responsibilities to other identities (see Adding delegations for identities on page 648) • Cancel delegations (see Canceling identity delegations on page 649) • Delete delegations (see Deleting identities' delegations on page 649)
Attestation	Opens the **Attestation – Identity** page (see Attestation – Identity (page description) on page 1389). You select the following actions: • Display all attestation cases linked to this identity (see Displaying identity attestation cases on page 650) • Display details of the objects being attested (see Displaying identity attestation cases on page 650) • Make approval decisions about pending attestation cases (see Approving and denying identity attestation cases on page 652) • Display attestors of pending attestation cases (see Displaying attestors of identity pending attestation cases on page 651) • Send reminders to approvers (see Sending reminders about identity pending attestation cases on page 654)
Risk	Opens the **Risk – Identity** page (see Risk – Identity (page description) on page 1391).

Tiles	Description
	You select the following actions: • Display the identity's calculated risk index (see Displaying identity risk indexes on page 655) • Show how the calculated risk index is put together
History	Opens the **History – Identity** page (see History – Identity (page description) on page 1392). Here you can view all identity changes (see Identity history on page 656).
Passcode	Here you can create a passcode for the identity in case it has forgotten its password to log in to Web Portal and cannot reset its password go to the question-and-answer function (see Creating passcodes for identities on page 659).

Overview – Identity (page description)

To open the **Overview - Identity** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity > **Overview**.

On the **Overview - Identity** page, you can see all the information relevant to the identity summarized in an overview (see Displaying identity overviews on page 643).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Identity (page description)

To open the **Main data - Identity** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity > **Main data**.

On the **Main data - Identity** page you can perform the following actions:

- Displaying and editing the identity's main data (see Displaying and editing identity main data on page 643)
- Transfer responsibility of the identity to another manager (see Assigning other managers to identities on page 644)
- Create reports on identity data (see Creating reports about identities on page 645)

The following tables give you an overview of the various features and content on the **Main data – Identity** page.

Table 829: Controls

Control	Description
Assign to new manager	This opens the **Assign to new manager** page . You can use this button to transfer the responsibility of the identity to another manager (see Assigning other managers to identities on page

Control	Description
	644).
Generate report	Opens a dialog. Use this button to generate a report about the identity's data (see Creating reports about identities on page 645).
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 830: Identities main data

Property	Description
Personal data	
Last name	Enter the identity's last name.
First name	Enter the identity's first name.
Middle name	Enter the identity's middle name.
Date of birth	Enter the identity's date of birth. Click the (**Calendar**) to do this and use the date picker to select the date of birth.
Personnel number	Enter the identity's personnel number.
Gender	In the menu, select the identity's gender.
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Organizational information	
Primary cost center	Click **Assign**/**Change** and select the identity's primary cost center.
Primary department	Click **Assign**/**Change** and select the identity's primary department.
External	Select the check box if this is an external identity.
Employee type	In the menu, select what type of identity this is. For example, an identity of this company or a trainee.
Entry date	Enter the date the identity started at the company. Click the (**Calendar**) and use the date picker to select the starting date.
Leaving date	Enter the date that the identity leaves the company. Click the (**Calendar**) to do this and use the date picker to select the leaving date.

Property	Description
Manager	Shows you the identity's manager. TIP: If necessary, you can transfer the identity's manager at a later date (see Assigning other managers to my identities on page 299).
Temporarily disable until	Select the check box to activate the identity at a later date then click the (**Calendar**) and use the date picker to select the date to activate the identity.
Locational information	
Primary location	Click **Assign**/**Change** and select the identity's primary location.
Building	Enter the building where the identity works.
Floor	Enter which floor the identity works on.
Room	Enter the room the identity works in.
Street	Enter the road where the identity works.
Zip code	Enter the zip code of the identity's work location.
City	Enter the city where the identity works.

Assigning to new manager (page description)

To open the **Assign to new manager** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity > **Main data** > **Assign to new manager**.

On the **Assign to New Manager** page, you can assign a new manager to an identity and specify which changes to make on the day the manager takes effect (see Assigning other managers to my identities on page 299).

NOTE: By default, if the identity to which you want to assign a new manager already has approved requests or entitlements, these will be deleted on the deadline by default. If you want the identity to retain these requests or entitlements when transferring to the new manager, disable the check box in the column **Delete on the effective date** or **Cancel on the effective date**.

The following tables give you an overview of the various features and content on the **Assign to New Manager** page.

Table 831: Controls

Control	Description
New manager	Click **Assign**/**Change** and then select the identity's new manager.
Effective date	Enter the date on which the new manager will take over responsibility for the identity. Click (**Calendar**) to do this and use the date picker to select the date.

Control	Description
Back	Opens the **Main data – Identity** page (see Main data – Identity (page description) on page 1020).
Submit	Use this button to save your settings. The manager will be assigned to the identity on the specified date.

Table 832: Columns

Column	Description
Description	Shows you which change is to be made on the effective date.
Object type	Shows you what type of object it is that will be changed on the effective date.
Object	Shows you the name of the object that will be changed on the effective date.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Requests - Identities ((page description))

To open the **Requests - Identities** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity > **Requests**.

On the **Requests - <identity>** page you can see all the products that this identity has requested or that have been requested for them (see Displaying identity requests on page 645).

The following tables give you an overview of the various features and content on the **Requests – <identity>** page.

Table 833: Controls

Control	Description
Advanced search	The advanced search allows you to control which product requests are displayed: • **Requests submitted by the selected identity for itself**: Select this check box to display product requests placed by the selected identity for themselves. • **Requests submitted by the selected identity for others**: Select this check box to display product requests placed by the selected identity for other identities. • **Requests submitted by others for the selected identity**: Select this check box to display product requests placed by other identities for the selected identity.

Control	Description
	• **Submitted requests in the selected identity's organization**: Select this check box to display product requests placed in the selected identity's scope of responsibility. • **Filter by request number**: Enter the request number of the request you want to display. • **pending**: Select this check box to display product requests that are not yet approved (status: **Request**). • **Approved**: Select this check box to display product requests that have been granted approval (status: **Assigned**). • **Canceled or denied or unsubscribed**: Select this check box to display product requests that have been canceled, denied, or unsubscribed. Click **Search** to apply the filter criteria to the request history. Click **Reset** to reset the filter criteria to the default search.

Table 834: Columns

Column	Description
Product	Shows the name of the product that was requested.
Status	Shows the current status of the product. The following status' are possible: • **Assigned**: The product request was successful and the product was successfully assigned. • **Request**: The product request is still awaiting an approval decision (it is still in the request workflow). In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Pending**: The product request is waiting for an approval decision from an approver. In the details pane, on the **Workflow** tab, you can see what the approval is waiting for. • **Approved**: The product request was granted approval by the approver and continues along the workflow. In the details pane, on the **Workflow** tab, you can see the current position in the workflow. • **Renewal**: The product has been renewed (see Renewing products with limit validity periods on page 130). • **Unsubscription**: The product is in the process of being unsubscribed (see Unsubscribing products on page 131). • **Denied**: The request for this product was denied. The reason for denying may be a policy or rule violation or the manager not verifying the request if it is only temporary. In the details pane, on the **Workflow** tab, you can see when and why the request was denied. .

Column	Description
	• **Canceled**: The product request was canceled or the system could not carry out the request (for example, because an identity for verifying it was not given or the validity period expired). In the details pane, on the **Workflow** tab, you can see when and why the request was canceled. • **Unsubscribed**: The product was unsubscribed (see Unsubscribing products on page 131). In the details pane, on the **Workflow** tab, you can see when and why the request was unsubscribed.
Request date	Shows when the product was requested. TIP: If you only want to display products that were requested within a certain time period, click **Filtering: Request date** next to the column header and select the appropriate options.
Recipient	Shows for whom the product was requested.
Shopping cart	Shows you the request number of the total request with which the product was requested.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

NOTE: On the following tabs, you can show other useful information about each product in the details pane. To do this, click the product in the list:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.

Entitlements – Identity (page description)

To open the **Entitlements - Identity** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity > **Entitlements**.

On the **Entitlements – Identity** page, you can:

- Display entitlements assigned to the identity (see Displaying identity entitlements on page 646)
- Remove the identity's entitlements (see Deleting identity entitlements on page 647)

TIP: Entitlements form the basis for membership in an object (for example in a department).

The following tables give you an overview of the various features and content on the **Entitlements – Identity** page.

Table 835: Controls

Control	Description
Deleting memberships	Use this button to delete selected entitlements (such as, membership in groups) (see Deleting identity entitlements on page 647). To do this, select the check box in front of the entitlement and click the button.

Table 836: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Object type	Shows you the entitlement type (for example, if it is a system role)
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Delegations – Identity (page description)

To open the **Delegations - Identity** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity > **Delegations**.

On the **Delegations – Identity** page, you can:

- Display all delegations that the identity is involved in (see Displaying identity delegations on page 648)
- Delegate the identity's role memberships and responsibilities to other identities (see Adding delegations for identities on page 648)
- Cancel delegations (see Canceling identity delegations on page 649)
- Delete delegations (see Deleting identities' delegations on page 649)

The following tables give you an overview of the various features and content on the **Delegations – Identity** page.

Table 837: Controls

Control	Description
Actions > Delete all delegations	Use this action to delete all existing delegations that the identity has triggered (see Deleting identities' delegations on page 649). NOTE: You cannot delete responsibilities that you have delegated to the identity here. Delete this delegation instead as described in Deleting delegations on page 461.
Actions > Delete	Use this action to delete delegations that you have previously selected

Control	Description
delegation	using the ☑ **Select** button (see Deleting identities' delegations on page 649).
Actions > Select all	Use this action to select all the delegations and then delete them (see Deleting identities' delegations on page 649).
New delegation	Use this button to add a new delegation (see Adding delegations for identities on page 648).

Table 838: Controls in the details pane of a delegation

Control	Description
Withdraw request	Use this button to cancel the selected delegation (see Canceling identity delegations on page 649).
Details	You can use this function to view details of all objects involved in the delegation (see Displaying identity delegations on page 648).

Table 839: Columns

Column	Description
Name	Shows you the name of the object whose responsibility has been delegated.
Delegator	Shows you the name of the identity that created the delegation.
Delegation recipient	Shows you the name of the identity to which the responsibility was delegated.
Criteria	Shows you what type of delegated responsibility it is. For example, if you delegate responsibility through an identity, the criteria is **Employee manager**.
Delete	Use the buttons to select delegations that you want to delete later using **Actions** > **Delete delegation**.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

TIP: You can view more information about each delegation on the tabs in the detail pane.

Attestation – Identity (page description)

To open the **Attestation – Identity** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity > **Attestation**.

On the **Attestation - Identity** page you can:

- Display all attestation cases linked to this identity (see Displaying identity attestation cases on page 650)
- Display details of the objects being attested (see Displaying identity attestation cases on page 650)
- Make approval decisions about pending attestation cases (see Approving and denying identity attestation cases on page 652)
- Display attestors of pending attestation cases (see Displaying attestors of identity pending attestation cases on page 651)
- Send reminders to approvers (see Sending reminders about identity pending attestation cases on page 654)

The following tables give you an overview of the various features and contents of the **Attestation – Identity** page.

Table 840: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of identity pending attestation cases on page 651) Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about identity pending attestation cases on page 654).
Approve	Opens the **Pending Attestations – Identity** page (see Pending attestations – Identity (page description) on page 932). Use this button to make approval decisions about attestation cases pending for the identity (see Approving and denying identity attestation cases on page 652).

Table 841: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of identity pending attestation cases on page 651) Then you can send reminder emails to these identities (see Sending reminders about identity pending attestation cases on page 654).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying identity attestation cases on page 650)

Table 842: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Identity (page description)

To open the **Risk – Identity** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity > **Risk**.

On the **Risk – Identity** page, you can:

- Display the identity's calculated risk index (see Displaying identity risk indexes on page 655)
- Show how the calculated risk index is put together

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the various features and content on the **Risk – Identity** page.

Table 843: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index.

Table 844: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Identity (page description)

To open the **History - Identity** page go to **Responsibilities** > **Governance Administration** > **Identities** > click an identity > **History**.

On the **History – Identity** page, you can display all the identity's changes (see Identity history on page 656).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows you all events concerning the identity, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the various features and content on the **History – Identity** page.

Table 845: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Disable this check box if you also want to see properties that have not changed since they were created.

Table 846: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 847: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	

Column	Description
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Multi-request resources (page description)

To open the **Multi-request resources** page go to **Responsibilities** > **Governance Administration** > **Multi-request resources**.

On the **Multi-request resources** page, you can see all multi-request resources (see Displaying multi-request resources on page 686).

If you click **Edit** in an multi-request resource's details pane, a new page opens, which contains more information and configuration options for the multi-request resource (see Multi-request resource (page description) on page 1395).

The following table gives you an overview of the various features and content on the **Multi-request resources** page.

Table 848: Columns

Column	Description
Display	Shows you the multi-request resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Multi-request resource (page description)

To open the **Multi-request resources** page go to **Responsibilities** > **Governance Administration** > **Multi-request resources** > **Edit**.

On the **Multi-request resource** page, you can perform various actions on the multi-request resource you selected beforehand.

To do this, click on one of the tiles:

Table 849: Tiles

Tiles	Description
Overview	Opens the **Overview - Multi-request resource** page (see Overview – Multi-request resource (page description) on page 1395). This provides you with all the information at a glance (see Displaying multi-request resource overviews on page 687). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Multi-request resource** page (see Main data – Multi-request resource (page description) on page 1396). Here you can view and edit the multi-request resource's main data (see Displaying and editing multi-request resources main data on page 687).
Attestation	Opens the **Attestation – Multi-request resource** page (see Attestation – Multi-request resource (page description) on page 1397). You select the following actions: • Display all attestation cases linked to this multi-request resource (see Displaying multi-request resource attestation cases on page 688) • Display details of the objects being attested (see Displaying multi-request resource attestation cases on page 688) • Make approval decisions about pending attestation cases (see Approving and denying multi-request resource attestation cases on page 691) • Display attestors of pending attestation cases (see Displaying attestors of multi-request resource pending attestation cases on page 690) • Send reminders to approvers (see Sending reminders about multi-request resource pending attestation cases on page 692)

Overview – Multi-request resource (page description)

To open the **Overview - Multi-request resource** page go to **Responsibilities** > **Governance Administration** > **Multi-request resources** > **Edit** > **Overview**.

On the **Overview – Multi-request resource** page, you can see all the information relevant to the multi-request resource summarized in an overview (see Displaying multi-request resource overviews on page 687).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Multi-request resource (page description)

To open the **Main data - Multi-request resources** page go to **Responsibilities** > **Governance Administration** > **Multi-request resources** > **Edit** > **Main data**.

On the **Main data - Multi-request resource** page, you can show and edit the multi-request resource's main data (see Displaying and editing multi-request resources main data on page 687).

The following tables give you an overview of the different functions and content on the **Main data – Multi-request resource** page.

Table 850: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 851: Multi-request resource main data

Property	Description
Multi-request resource	Enter a full, descriptive name for the multi-request resource.
Resource type	Select the resource type of the multi-request resource. Use resource types to group multi-request resources.
Description	Enter a description for the multi-request resource.
IT Shop	Select the check box if the multi-request resource can also be requested through the IT Shop. This multi-request resource can be requested by your identities using the Web Portal and granted through a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the multi-request resource can only be requested through the IT Shop. This multi-request resource can be requested by your identities using the Web Portal and granted through a defined approval process. It is not possible to assign a multi-request resource directly to roles outside of the IT Shop (for example in the Manager).
Service item	Click **Create a new service item** and create a new service item (a

Property	Description
	product). If a service item is already assigned, click **Change** and select a service item. You cannot use an multi-request resource until a service item has been assigned to it.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning multi-request resources to identities. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Attestation – Multi-request resource (page description)

To open the **Attestation - Multi-request resource** page go to **Responsibilities** > **Governance Administration** > **Multi-request resources** > **Edit** > **Attestation**.

On the **Attestation - Multi-request resource** page you can:

- Display all attestation cases linked to this multi-request resource (see Displaying multi-request resource attestation cases on page 688)
- Display details of the objects being attested (see Displaying multi-request resource attestation cases on page 688)
- Make approval decisions about pending attestation cases (see Approving and denying multi-request resource attestation cases on page 691)
- Display attestors of pending attestation cases (see Displaying attestors of multi-request resource pending attestation cases on page 690)
- Send reminders to approvers (see Sending reminders about multi-request resource pending attestation cases on page 692)

The following tables give you overview of the various features and contents of the **Attestation – Multi-request resource** page.

Table 852: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about multi-request resource pending attestation cases on page 692).
Approve	Opens the **Pending Attestations – Multi-request resources** (see Pending attestation – Multi-request resource (page description) on

Control	Description
	page 955). Use this button to make approval decisions about attestation cases pending for the multi-request resource (see Approving and denying multi-request resource attestation cases on page 691).

Table 853: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case Then you can send reminder emails to these identities (see Sending reminders about multi-request resource pending attestation cases on page 692).
Show details	You can use this button to display details about all the objects that are included in this attestation case

Table 854: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Multi requestable/unsubscribable resources (page description)

You can open the **Multi requestable/unsubscribable resources** page go to **Responsibilities** > **Governance Administration** > **Multi requestable/unsubscribable resources**.

On the **Multiple requestable/unsubscribable resources** page, you can see all the multiple requestable/unsubscribable resources (see Displaying all multi requestable/unsubscribable resources on page 694).

If you click **Edit** in an multiple requestable/unsubscribable resource's details pane, a new page opens, which contains more information and configuration options for the multiple requestable/unsubscribable resource (see Multi requestable/unsubscribable resource (page description) on page 1399).

The following table gives you an overview of the various features and content on the **Multi requestable/unsubscribable resources** page.

Table 855: Columns

Column	Description
Display	Shows you the multi requestable/unsubscribable resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Multi requestable/unsubscribable resource (page description)

To open the **Multi requestable/unsubscribable resource** page go to **Responsibilities** > **Governance Administration** > **Multi requestable/unsubscribable resource** > **Edit**.

On the **Multi requestable/unsubscribable resource** page, you can perform various actions on the multi requestable/unsubscribable resource you selected beforehand.

To do this, click on one of the tiles:

Table 856: Tiles

Tiles	Description
Overview	Opens the **Overview - Multi requestable/unsubscribable resource** page (see Overview – Multi requestable/unsubscribable resource (page description) on page 1401). This provides you with all the information at a glance (see Displaying multi requestable/unsubscribable resource overviews on page 695). For

Tiles	Description
	more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Multi requestable/unsubscribable resource** page (see Main data – Multi requestable/unsubscribable resource (page description) on page 1401). Here you can view and edit the multi-requestable/unsubscribable resource's main data (see Displaying and editing multi-request resources main data on page 687).
Memberships	Opens the **Memberships - Multi requestable/unsubscribable resource** page (see Memberships – Multi requestable/unsubscribable resource (page description) on page 1402). You select the following actions: • Display identities that are assigned this multi requestable/unsubscribable resource (see Displaying multi requestable/unsubscribable resource memberships on page 696) • Request this multi requestable/unsubscribable resource for identities (see Assigning identities to multi requestable/unsubscribable resources on page 697) • Cancel this multi requestable/unsubscribable resource for identities (see Removing multi requestable/unsubscribable resources from identities on page 698)
Attestation	Opens the **Attestation – Multi requestable/unsubscribable resource** page (see Attestation – Multi requestable/unsubscribable resource (page description) on page 1403). You select the following actions: • Display all attestation cases linked to this multi requestable/unsubscribable resource (see Displaying multi requestable/unsubscribable resource attestation cases on page 699) • Display details of the objects being attested (see Displaying multi requestable/unsubscribable resource attestation cases on page 699) • Make approval decisions about pending attestation cases (see Approving and denying multi requestable/unsubscribable resource attestation cases on page 702) • Display attestors of pending attestation cases (see Displaying attestors of multi requestable/unsubscribable resource pending attestation cases on page 700) • Send reminders to approvers (see Sending reminders about multi requestable/unsubscribable resource pending attestation cases on page 703)

Overview – Multi requestable/unsubscribable resource (page description)

To open the **Overview – Multi requestable/unsubscribable resource** page go to **Responsibilities** > **Governance Administration** > **Multi requestable/unsubscribable resources** > **Edit** > **Overview**.

On the **Overview – Multi requestable/unsubscribable resource** page, you can see all the information relevant to the multi requestable/unsubscribable resource summarized in an overview (see Displaying multi requestable/unsubscribable resource overviews on page 695).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Multi requestable/unsubscribable resource (page description)

To open the **Main data - Multi requestable/unsubscribable resource** page go to **Responsibilities** > **Governance Administration** > **Multi requestable/unsubscribable resource** > **Edit** > **Main data**.

On the **Main data - Multi requestable/unsubscribable resource** page, you can show and edit the ulti requestable/unsubscribable resource's main data (see Displaying and editing multi-request resources main data on page 687).

The following tables give you an overview of the different functions and content on the **Main data – Multi requestable/unsubscribable resource** page.

Table 857: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 858: Multi requestable/unsubscribable resource main data

Property	Description
Multi requestable/unsubscribable resource	Enter a full, descriptive name for the multi requestable/unsubscribable resource.
Resource type	Select the resource type of the multi requestable/unsubscribable resource. Use resource types to group multi requestable/unsubscribable resources.
Description	Enter a description for the multi requestable/unsubscribable resource.

Property	Description
IT shop	Select the check box if the multi requestable/unsubscribable resource can also be requested through the IT Shop. This multi requestable/unsubscribable resource can be requested by your identities using the Web Portal and granted through a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the multi requestable/unsubscribable resource can only be requested through the IT Shop. This multi requestable/unsubscribable resource can be requested by your identities using the Web Portal and granted through a defined approval process. It is not possible to assign a multi requestable/unsubscribable resource directly to roles outside of the IT Shop (for example in the Manager).
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use an multi requestable/unsubscribable resource until a service item has been assigned to it.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning multi requestable/unsubscribable resources to identities. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Memberships – Multi requestable/unsubscribable resource (page description)

- Display identities that are assigned this multi requestable/unsubscribable resource (see Displaying multi requestable/unsubscribable resource memberships on page 696)
- Request this multi requestable/unsubscribable resource for identities (see Assigning identities to multi requestable/unsubscribable resources on page 697)
- Cancel this multi requestable/unsubscribable resource for identities (see Removing multi requestable/unsubscribable resources from identities on page 698)

Table 859: Controls

Control	Description
Request memberships	
Delete memberships	

Table 860: Columns

Column	Description
Identity	
Origin	

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Multi requestable/unsubscribable resource (page description)

To open the **Attestation - Multi requestable/unsubscribable resource** page go to **Responsibilities** > **Governance Administration** > **Multi requestable/unsubscribable resources** > **Edit** > **Attestation**.

On the **Attestation - Multi requestable/unsubscribable resource** page you can:

- Display all attestation cases linked to this multi requestable/unsubscribable resource (see Displaying multi requestable/unsubscribable resource attestation cases on page 699)
- Display details of the objects being attested (see Displaying multi requestable/unsubscribable resource attestation cases on page 699)
- Make approval decisions about pending attestation cases (see Approving and denying multi requestable/unsubscribable resource attestation cases on page 702)

- Display attestors of pending attestation cases (see Displaying attestors of multi requestable/unsubscribable resource pending attestation cases on page 700)
- Send reminders to approvers (see Sending reminders about multi requestable/unsubscribable resource pending attestation cases on page 703)

The following tables give you an overview of the various features and contents of the **Attestation – Multi requestable/subscribable resource** page.

Table 861: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about multi requestable/unsubscribable resource pending attestation cases on page 703).
Approve	Opens the **Pending Attestations – Multi requestable/un-subscribable resources** (see Pending attestations: Multi requestable/unsubscribable resources (page description) on page 962). Use this button to make approval decisions about attestation cases pending for the multi requestable/unsubscribable resource (see Approving and denying multi requestable/unsubscribable resource attestation cases on page 702).

Table 862: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case Then you can send reminder emails to these identities (see Sending reminders about multi requestable/unsubscribable resource pending attestation cases on page 703).
Show details	You can use this button to display details about all the objects that are included in this attestation case

Table 863: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation	Shows the name of the attestation policy in use.

Column	Description
policy	
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Organization (page description)

To open the **Organization** page go to **Responsibilities** > **Governance Administration** > **Organization**.

On the **Organization** page, you can select from the **Type** drop-down menu:

- Display all departments (see Displaying all departments on page 591)
- Restore deleted departments (see Restoring deleted departments on page 591)
- Display all cost centers (see Displaying all cost centers on page 660)
- Restore deleted cost centers (see Restoring deleted cost centers on page 661)
- Display all locations (see Displaying all locations on page 716)
- Restore deleted locations (see Restoring deleted locations on page 716)

If you click **Edit** in the details pane of a department, cost center, or location, a new page opens, which contains more information and configuration options for the department (see Department (page description) on page 1406), cost center (see Cost center (page description) on page 1419), or the location (see Location (page description) on page 1431).

The following tables give you an overview of the various features and content on the **Devices** page.

Table 864: Controls

Control	Description
Type	You can use this drop-down menu to select whether you display departments, cost centers or locations.
To restore a deleted role	You can use this button to restore a deleted department (see Restoring deleted departments on page 591), cost center (see Restoring deleted cost centers on page 661), or location (see Restoring deleted locations on page 716).

Table 865: Columns

Column	Description
Display	Shows you the name of the department, cost center, or location.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Department (page description)

To open the **Department** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit**.

On the **Department** page, you can perform various actions on the department you selected beforehand.

To do this, click on one of the tiles:

Table 866: Tiles

Tiles	Description
Overview	Opens the **Overview - Department** page (see Overview – Department (page description) on page 1408) This provides you with all the information at a glance (see Displaying department overviews on page 592). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Department** page (see Main data – Department (page description) on page 1408). Here you can display and edit the department's main data (see Displaying and editing department main data on page 593).
Memberships	Opens the **Memberships - Department** page (see Memberships – Department (page description) on page 1410). You select the following actions: • Display identities that are assigned this department (see

Tiles	Description
	Displaying department memberships on page 594) • Assign identities to the department (see Assigning identities to departments on page 594) • Remove identities from the department (see Removing identities from departments on page 595)
Permissions	Opens the **Entitlements – Department** page (see Entitlements – Department (page description) on page 1411) You select the following actions: • Display entitlements assigned to this department (see Displaying department entitlements on page 596) • Add new entitlements to the department (see Adding department entitlements on page 597) • Delete department entitlements (see Deleting department entitlements on page 598)
Attestation	Opens the **Attestations – Department** page (see Attestation – Department (page description) on page 1412). You select the following actions: • Display all attestation cases linked to this department (see Displaying department attestation cases on page 602) • Display details of the objects being attested (see Displaying department attestation cases on page 602) • Make approval decisions about pending attestation cases (see Approving and denying department attestation cases on page 605) • Display attestors of pending attestation cases (see Displaying attestors of department pending attestation cases on page 604) • Send reminders to approvers (see Sending reminders about department pending attestation cases on page 606)
Risk	Opens the **Risk – Department** page (see Risk – Department (page description) on page 1414) You select the following actions: • Display the department's calculated risk index (see Displaying department risk indexes on page 608) • Show how the calculated risk index is put together
History	Opens the **History – Department** page (see History – Department (page description) on page 1415)

Tiles	Description
	Here you can see all the changes made to the department (see Department history on page 609).
Usage	Opens the **Usage – Department** page (see Usage – Department (page description) on page 1417) Here you can display which roles the members of the department belong to (see Displaying role memberships of department members on page 612).
Compliance reports	Opens the **Compliance report – Department** page (see Compliance reports – Department (page description) on page 1417). You select the following actions: • Display the department's policy violations (see Displaying department policy violations on page 600) • Display rule violations of department members (see Displaying rule violations of department members on page 600) • Display risk indexes and entitlements of department members (see Displaying risk indexes and entitlements of department members on page 601)
Split	Here you can divide the department into two sections (see Copying/splitting departments on page 613).
Compare and merge	Here you can compare and merge the department with another role (department, business role, cost center or location) (see Comparing and merging departments on page 614).
Redo	Here you can restore a deleted department that was under this department (see Restoring deleted departments on page 591).
Statistics	Here you can see various statistics about the department (see Displaying department statistics on page 616).

Overview – Department (page description)

Open the **Overview – Department** page by navigating through **Responsibilities** > **Governance Administration** > **Departments** > **Edit** > **Overview**.

On the **Overview – Department** page, you can see all the information relevant to the department summarized in an overview (see Displaying department overviews on page 592).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Department (page description)

To open the **Overview – Department** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Main data**.

On the **Main data - Department** page, you can show and edit the department's main data (see Displaying and editing department main data on page 593).

The following tables give you an overview of the different functions and content on the **Main data – Department** page.

Table 867: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 868: Department main data

Property	Description
Department	Enter a full, descriptive name for the department.
Short name	Enter a short name for the department.
Object ID	Enter a unique object ID for the department. For example, the object ID is required in SAP systems for assigning identities to departments.
Parent department	Click **Assign**/**Change** and select a department to be the parent department for organizing the department hierarchically. If you want the department at the root of a department hierarchy, leave the field empty.
Manager	Click **Assign**/**Change** and select the manager responsible for the department.
2nd Manager	Click **Assign**/**Change** and select an identity to act as a deputy to the department's manager.
Location	Click **Assign**/**Change** and select the location the cost center is primarily assigned to.
Attestors	Click **Assign**/**Change** and select a cost center. Members of the selected application role can approve attestation cases for the department.
Cost center	Click **Assign**/**Change** and select the location the department is primarily assigned to.
Role approver	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the department.
Role approver (IT)	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the department.
Description	Enter a description for the department.

Memberships – Department (page description)

To open the **Memberships – Department** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Memberships**.

On the **Memberships – Department** page, you can:

- Display identities that are assigned this department (see Displaying department memberships on page 594)
- Assign identities to the department (see Assigning identities to departments on page 594)
- Remove identities from the department (see Removing identities from departments on page 595)

The following tables give you an overview of the different functions and content on the **Memberships – Department** page.

Table 869: Controls

Control	Description
Request memberships	Use this button to request membership in the department for identities (see Assigning identities to departments on page 594).
Delete member-ships	You can remove selected identities from the department using this button (see Removing identities from departments on page 595). Select the check boxes in front of the identities you want to remove from the department and click this button.

Table 870: Columns

Column	Description
Identity	Shows you the name of the identity assigned to the department.
Origin	Shows you whether the department of the identity was assigned directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Department (page description)

To open the **Entitlements - Department** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Entitlements**.

On the **Entitlements – Department** page, you can:

- Display entitlements assigned to this department (see Displaying department entitlements on page 596)
- Add new entitlements to the department (see Adding department entitlements on page 597)
- Delete department entitlements (see Deleting department entitlements on page 598)

TIP: Entitlements form the basis for membership in an object (for example in a department).

The following tables give you an overview of the various features and content on the **Entitlements – Department** page.

Table 871: Controls

Control	Description
New	Use this button to add a new entitlement to the department (see Adding department entitlements on page 597). Identities that this department is assigned to, automatically obtain membership in the object assigned here.
Remove	You can use this button to delete selected permissions (see Deleting business role entitlements on page 624)(see Deleting department entitlements on page 598)(see Deleting cost center entitlements on page 667)(see Deleting entitlements from locations on page 723). To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 872: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Department (page description)

To open the **Compliance - Department** page go to **Responsibilities** > **Governance Administration** > **Departments** > **Edit** > **Compliance**.

On the **Compliance - Department** page, you can view compliance rule violations caused by the department (see Displaying department rule violations on page 599).

The following table gives an overview of the different content on the **Compliance – Department** page.

Table 873: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Department (page description)

To open the **Attestation - Department** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Attestation**.

On the **Attestation - Department** page you can:

- Display all attestation cases linked to this department (see Displaying department attestation cases on page 602)
- Display details of the objects being attested (see Displaying department attestation cases on page 602)
- Make approval decisions about pending attestation cases (see Approving and denying department attestation cases on page 605)

- Display attestors of pending attestation cases (see Displaying attestors of department pending attestation cases on page 604)
- Send reminders to approvers (see Sending reminders about department pending attestation cases on page 606)

The following tables give you overview of the various features and contents of the **Attestation – Department** page.

Table 874: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see Displaying attestors of department pending attestation cases on page 604)Displaying attestors of cost center pending attestation cases on page 673 Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about department pending attestation cases on page 606).
Approve	Opens the **Pending Attestations – Department** (see Pending attestations – Department (page description) on page 909) Use this button to make approval decisions about attestation cases pending for the department (see Approving and denying department attestation cases on page 605).

Table 875: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see Displaying attestors of department pending attestation cases on page 604) Then you can send reminder emails to these identities (see Sending reminders about department pending attestation cases on page 606).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see Displaying department attestation cases on page 602)

Table 876: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.

Column	Description
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Department (page description)

To open the **Risk – Department** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Risk**.

On the **Risk – Department** page, you can:

- Display the department's calculated risk index (see Displaying department risk indexes on page 608)
- Show how the calculated risk index is put together

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the various features and content on the **Risk – Department** page.

Table 877: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index.

Table 878: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Department (page description)

To open the **History - Department** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **History**.

On the **History – Department** page, you can see all the changes made to the department (see Department history on page 609).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows you all the events, which affect a department, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Department** page.

Table 879: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user.

Control	Description
	TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Disable this check box if you also want to see properties that have not changed since they were created.

Table 880: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 881: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.

Column	Description
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Department (page description)

To open the **Usage - Department** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Usage**.

On the **Usage - Department** page you can see which roles the department members belong to (see Displaying role memberships of department members on page 612).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the different functions on the **Usage – System role** page.

Table 882: Controls

Control	Description
Role classes	You can select the main category of roles and organizations you want to display from this menu.
More information	Use this button to show the legend that explains the content of the overview.

Compliance reports – Department (page description)

To open the **Compliance Reports – Department** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Compliance Reports**.

On the **Compliance Reports – Department** page you can:

- Display the department's policy violations (see Displaying department policy violations on page 600)
- Display rule violations of department members (see Displaying rule violations of department members on page 600)
- Display risk indexes and entitlements of department members (see Displaying risk indexes and entitlements of department members on page 601)

The information is divided into three parts:

- **Policy violations**: Shows all the current policy violations caused by the department.
- **Compliance rule violations**: Shows you the current rule violations of the identities to which the department is assigned.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and entitlements**: Displays all identities to which the department is assigned. In addition, the number of entitlements and risk index assigned to these identities is displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – Department** page.

Table 883: Columns

Column	Description
Policy violations	
Violating object	Show which object caused the rule violation.
Policy	Show the policy that was violated.
Status	Show the status of the rule policy.
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows the violated rule.
Approval state	Shows how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

Column	Description
Identities: Risk index and entitlements	
Identity	Shows you the identity to which this department is assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Cost center (page description)

To open the **Cost Center** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit**.

On the **Cost center** page, you can perform various actions on the cost center you selected beforehand.

To do this, click on one of the tiles:

Table 884: Tiles

Tiles	Description
Overview	Opens the **Overview - Cost center** page (see Overview – Cost center (page description) on page 1421). This provides you with all the information at a glance (see Displaying cost center overviews on page 662). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Cost center** page (see Main data – Cost center (page description) on page 1421). Here you can display and edit the cost center's main data (see Displaying and editing cost center main data on page 662).
Memberships	Opens the **Memberships - Cost center** page (see Memberships – Cost center (page description) on page 1422). You select the following actions: • Display identities that are assigned this location (see Displaying cost center memberships on page 663) • Assign identities to the location (see Assigning identities to cost centers on page 664) • Remove identities from the location (see Removing identities from cost centers on page 665)
Permissions	Opens the **Entitlements – Cost center** page (see Entitlements –

Tiles	Description
	Department (page description) on page 1411). You select the following actions: • Display entitlements assigned to the cost center (see Displaying cost center entitlements on page 666) • Add new entitlements to the cost center (see Adding cost center entitlements on page 666) • Delete cost center entitlements (see Deleting cost center entitlements on page 667)
Attestation	Opens the **Attestation – Cost center** page (see Attestation – Cost center (page description) on page 1425). You select the following actions: • Display all attestation cases linked to this cost center (see Displaying cost center attestation cases on page 672) • Display details of the objects being attested (see Displaying cost center attestation cases on page 672) • Make approval decisions about pending attestation cases (see Approving and denying cost center attestation cases on page 674) • Display attestors of pending attestation cases (see Displaying attestors of cost center pending attestation cases on page 673) • Send reminders to approvers (see Sending reminders about cost center pending attestation cases on page 676)
Risk	Opens the **Risk – Cost center** page (see Risk – Cost center (page description) on page 1427). You select the following actions: • Display the cost center's calculated risk index (see Displaying cost center risk indexes on page 677) • Show how the calculated risk index is put together
History	Opens the **History – Cost center** page (see History – Cost center (page description) on page 1428). Here you can see all the changes made to the cost center (see Cost center history on page 678).
Usage	Opens the **Usage – Cost center** page (see Usage – Cost center (page description) on page 1430). Here you can display which roles the members of the cost center belong to (see Displaying role memberships of cost center members on page 682).

Tiles	Description
Compliance reports	Opens the **Compliance report – Cost center** page (see Compliance reports – Cost center (page description) on page 1430). You select the following actions: • Display the cost center's policy violations (see Displaying cost center policy violations on page 669) • Display rule violations of system role members (see Displaying rule violations of cost center members on page 670) • Display risk indexes and entitlements of the cost center members (see Displaying risk indexes and entitlements of cost center members on page 670)
Split	Here you can split the cost center into two cost centers (see Copying/splitting cost centers on page 682).
Compare and merge	Here you can compare and merge the cost center with another role (cost center, business role, department or location) (see Comparing and merging cost centers on page 684).
Redo	Here you can restore a deleted cost center that was under this cost center (see Restoring deleted cost centers on page 661).
Statistics	Here you can see various statistics about the cost center (see Displaying cost center statistics on page 685).

Overview – Cost center (page description)

Open the **Overview – Cost center** page by navigating through **Responsibilities** > **Governance Administration** > **Cost centers** > **Edit** > **Overview**.

On the **Overview – Cost center** page, you can display all the information relevant to the cost center summarized in an overview (see Displaying cost center overviews on page 662.)

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Cost center (page description)

To open the **Overview – Cost center** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Main data**.

On the **Main data - Cost center** page, you can show and edit the cost center's main data (see Displaying and editing cost center main data on page 662).

The following tables give you an overview of the different functions and content on the **Main data – Cost center** page.

Table 885: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 886: Cost center main data

Property	Description
Cost center	Enter a full, descriptive name for the cost center.
Short name	Enter a short name for the cost center.
Parent cost center	Click **Assign**/**Change** and select a cost center to be the parent cost center for organizing the cost center hierarchically. If you want the cost center at the root of a cost center hierarchy, leave the field empty.
Manager	Click **Assign**/**Change** and select the manager responsible for the cost center.
2nd Manager	Click **Assign**/**Change** and select an identity to act as a deputy to the cost center's manager.
Attestors	Click **Assign**/**Change** and select a cost center. Members of the selected application role can approve attestation cases for the cost center.
Department	Click **Assign**/**Change** and select the department that the cost center is primarily assigned to.
Location	Click **Assign**/**Change** and select the location the cost center is primarily assigned to.
Role approver	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the cost center.
Role approver (IT)	Click **Assign**/**Change** and select an application role. Members of the selected application role can approve requests for members of the cost center.
Description	Enter a description for the cost center.

Memberships – Cost center (page description)

To open the **Memberships – Cost center** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Memberships**.

On the **Memberships – Cost center** page, you can:

- Display identities that are assigned this location (see Displaying cost center memberships on page 663)
- Assign identities to the location (see Assigning identities to cost centers on page 664)

- Remove identities from the location (see Removing identities from cost centers on page 665)

The following tables give you an overview of the different functions and content on the **Memberships – Cost center** page.

Table 887: Controls

Control	Description
Request memberships	Use this button to request membership in the cost center for identities (see Assigning identities to cost centers on page 664).
Delete memberships	You can use this button to remove selected identities from the cost center (see Removing identities from cost centers on page 665). Select the check boxes in front of the identities you want to remove from the cost center and click this button.

Table 888: Columns

Column	Description
Identity	Shows you the name of the identity assigned to the cost center.
Origin	Shows you whether the cost center of the identity was assigned directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Cost center (page description)

To open the **Entitlements - Cost Center** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Entitlements**.

On the **Entitlements – Cost center** page, you can:

- Display entitlements assigned to the cost center (see Displaying cost center entitlements on page 666)
- Add new entitlements to the cost center (see Adding cost center entitlements on page 666)
- Delete cost center entitlements (see Deleting cost center entitlements on page 667)

TIP: Entitlements form the basis for membership in an object (for example in a department).

The following tables give you an overview of the various features and content on the **Entitlements – Cost center** page.

Table 889: Controls

Control	Description
New	Use this button to add a new entitlement to the cost center (see Adding cost center entitlements on page 666). Identities that this cost center is assigned to, automatically obtain membership in the object assigned here.
Remove	You can use this button to delete selected permissions (see Deleting business role entitlements on page 624)(see Deleting department entitlements on page 598)(see Deleting cost center entitlements on page 667)(see Deleting entitlements from locations on page 723). To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 890: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Cost center (page description)

To open the **Compliance - Cost Center** page go to **Responsibilities** > **Governance Administration** > **Cost Centers** > **Edit** > **Compliance**.

On the **Compliance - Cost center** page, you can view compliance rule violations caused by the cost center (see Displaying cost center rule violations on page 669).

The following table gives an overview of the different content on the **Compliance – Cost center** page.

Table 891: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Cost center (page description)

To open the **Attestation - Cost Center** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Attestation**.

On the **Attestation - Cost Center** page you can:

- Display all attestation cases linked to this cost center (see Displaying cost center attestation cases on page 672)
- Display details of the objects being attested (see Displaying cost center attestation cases on page 672)
- Make approval decisions about pending attestation cases (see Approving and denying cost center attestation cases on page 674)
- Display attestors of pending attestation cases (see Displaying attestors of cost center pending attestation cases on page 673)
- Send reminders to approvers (see Sending reminders about cost center pending attestation cases on page 676)

The following tables give you an overview of the various features and contents of the **Attestation – Cost Center** page.

Table 892: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases (see . Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about cost center pending attestation cases on page 676).
Approve	Opens the **Pending Attestations – Cost center** (see Pending attestations – Cost center (page description) on page 935). Use this button to make approval decisions about attestation cases pending for the cost center (see Approving and denying cost center attestation cases on page 674).

Table 893: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case (see .Displaying attestors of cost center pending attestation cases on page 673 Then you can send reminder emails to these identities (see Sending reminders about cost center pending attestation cases on page 676).
Show details	You can use this button to display details about all the objects that are included in this attestation case (see .Displaying cost center attestation cases on page 672

Table 894: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on

Column	Description
	the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Cost center (page description)

To open the **Risk – Cost center** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Risk**.

On the **Risk – Cost center** page, you can:

- Display the cost center's calculated risk index (see Displaying cost center risk indexes on page 677)
- Show how the calculated risk index is put together

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the various features and content on the **Risk – Cost center** page.

Table 895: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index.

Table 896: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Cost center (page description)

To open the **History - Cost Center** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **History**.

On the **History – Cost center** page, you can see all the changes made to the cost center (see Cost center history on page 678).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows you all the events, which affect a cost center, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Cost center** page.

Table 897: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Disable this check box if you also want to see properties that have not changed since they were created.

Table 898: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 899: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Cost center (page description)

To open the **Usage - Cost Center** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Usage**.

On the **Usage - Cost Center** page, you can see which roles the cost center members belong to (see Displaying role memberships of cost center members on page 682).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the different functions on the **Usage – Cost center** page.

Table 900: Controls

Control	Description
Role classes	You can select the main category of roles and organizations you want to display from this menu.
More information	Use this button to show the legend that explains the content of the overview.

Compliance reports – Cost center (page description)

To open the **Compliance Reports – Cost Center** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Compliance Reports**.

On the **Compliance Reports – Cost center** page you can:

- Display the cost center's policy violations (see Displaying cost center policy violations on page 669)
- Display rule violations of system role members (see Displaying rule violations of cost center members on page 670)
- Display risk indexes and entitlements of the cost center members (see Displaying risk indexes and entitlements of cost center members on page 670)

The information is divided into three parts:

- **Policy violations**: Shows all the current policy violations caused by the cost center.
- **Compliance rule violations**: Shows you all current rule violations of the identities assigned to the cost center.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and entitlements**: Displays all identities to which the cost center is assigned. In addition, the number of entitlements and risk index assigned to these identities is displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – Cost center** page.

Table 901: Columns

Column	Description
Policy violations	
Violating object	Show which object caused the rule violation.
Policy	Show the policy that was violated.
Status	Show the status of the rule policy.
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows the violated rule.
Approval state	Shows how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.
Identities: Risk index and entitlements	
Identity	Shows you the identity to which to the cost center is assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Location (page description)

To open the **Location** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit**.

On the **Location** page, you can perform various actions on the location you selected.

To do this, click on one of the tiles:

Table 902: Tiles

Tiles	Description
Overview	Opens the **Overview – Location** page (see Overview - Location (page

Tiles	Description
	description) on page 1434). This provides you with all the information at a glance (see Displaying location overviews on page 717). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Location** page (see Main data - Location (page description) on page 1434). Here you can see and edit the location's main data (see Displaying and editing location main data on page 718).
Memberships	Opens the **Memberships - Location** page (see Memberships – Location (page description) on page 1435). You select the following actions: • Display identities assigned to the location (see Displaying location memberships on page 719) • Assign identities to the location (see Assigning identities to locations on page 720) • Remove identities from the location (see Removing identities from locations on page 720)
Permissions	Opens the **Entitlements – Location** page (see Entitlements – Location (page description) on page 1436). You select the following actions: • Display entitlements assigned to the location (see Displaying location entitlements on page 721) • Add new entitlements to the location (see Adding location entitlements on page 722) • Delete the location's entitlements/memberships (see Deleting entitlements from locations on page 723)
Attestation	Opens the **Attestation – Location** page (see Attestation – Location (page description) on page 1438). You select the following actions: • Display all attestation cases linked to this location (see Displaying location attestation cases on page 727) • Display details of the objects being attested (see Displaying location attestation cases on page 727) • Make approval decisions about pending attestation cases (see Approving and denying location attestation cases on page 730) • Display attestors of pending attestation cases (see Displaying attestors of location pending attestation cases on page 729)

Tiles	Description
	• Send reminders to approvers (see Sending reminders about location pending attestation cases on page 731)
Risk	Opens the **Risk – Location** page (see Risk – Location (page description) on page 1439). You select the following actions: • Display the location's calculated risk index (see Displaying location risk indexes on page 733) • Show how the calculated risk index is put together
History	Opens the **History – Location** page (see History – Location (page description) on page 1440). Here you can view all changes made to the location (see Location history on page 734).
Usage	Opens the **Usage – Location** page (see Usage – Location (page description) on page 1442). Here you can display which roles the members of the site belong to (see Displaying role memberships of location members on page 737).
Compliance reports	Opens the **Compliance report – Location** page (see Compliance reports - Location (page description) on page 1443). You select the following actions: • Display the location's policy violations (see Displaying location policy violations on page 725) • Display rule violations of location members (see Displaying rule violations of location members on page 725) • Display risk indexes and entitlements of location members (see Displaying risk indexes and entitlements of location members on page 726)
Split	Here you can split the site into two locations (see Copying/splitting locations on page 738).
Compare and merge	Here you can compare and merge the location with another role (location, business role, department or cost center) (see Comparing and merging locations on page 739).
Redo	Here you can restore a deleted location that was under this location (see Restoring deleted locations on page 716).
Statistics	Here you can see various statistics about the location (see Displaying location statistics on page 741).

Overview - Location (page description)

Open the **Overview – Location** page by navigating through **Responsibilities** > **Governance Administration** > **Locations** > **Edit** > **Overview**.

On the **Overview - Location** page, you can see all the information relevant to the location summarized in an overview (see Displaying location overviews on page 717).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data - Location (page description)

To open the **Main data - Location** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Main data**.

On the **Main data - Location** page you can view and edit the master data of the location (see Displaying and editing location main data on page 718).

The following tables give you an overview of the different functions and content on the **Main data – Location** page.

Table 903: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 904: Location main data

Property	Description
Location	Enter a full, descriptive name for the location.
Short name	Enter a short name for the location.
Name	Enter an additional description for the location.
Parent location	Click **Assign**/**Change** and select a location to be the parent location for organizing the location hierarchically. If you want the location at the root of a location hierarchy, leave the field empty.
Manager	Click **Assign**/**Change** and select the manager responsible for the location.
2nd Manager	Click **Assign**/**Change** and select an identity to act as a deputy to the location's manager.
Attestors	Click **Assign**/**Change** and select a cost center. Members of the selected application role can approve attestation cases for the location.
Department	Click **Assign**/**Change** and select the department the location is primarily assigned to.

Property	Description
Cost center	Click **Assign/Change** and select the cost center the location is primarily assigned to.
Role approver	Click **Assign/Change** and select an application role. Members of the selected application role can approve requests for members of the location.
Role approver (IT)	Click **Assign/Change** and select an application role. Members of the selected application role can approve requests for members of the location.
Description	Enter a description for the location.

Memberships – Location (page description)

To open the **Memberships – Location** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Memberships**.

On the **Memberships – Location** page, you can:

- Display identities assigned to the location (see Displaying location memberships on page 719)
- Assign identities to the location (see Assigning identities to locations on page 720)
- Remove identities from the location (see Removing identities from locations on page 720)

The following tables give you an overview of the different functions and content on the **Memberships – Location** page.

Table 905: Controls

Control	Description
Request memberships	Use this button to request in the location assignment for identities (see Assigning identities to locations on page 720).
Delete memberships	You can use this button to delete the assignment to the location for selected identities (see Removing identities from locations on page 720). Select the check boxes in front of the identities whose locations you want to delete and click this button.

Table 906: Columns

Column	Description
Identity	Shows you the name of the identity assigned to the location.
Origin	Shows you whether the location of the identity was assigned directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – Location (page description)

To open the **Entitlements - Location** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Entitlements**.

On the **Entitlements – Location** page, you can:

- Display entitlements assigned to the location (see Displaying location entitlements on page 721)
- Add new entitlements to the location (see Adding location entitlements on page 722)
- Delete the location's entitlements/memberships (see Deleting entitlements from locations on page 723)

TIP: Entitlements form the basis for membership in an object (for example in a department).

The following tables give you an overview of the various features and content on the **Entitlements – Location** page.

Table 907: Controls

Control	Description
New	Use this button to add a new entitlement to the location (see Adding location entitlements on page 722). Identities that this location is assigned to, automatically obtain membership in the object assigned here.
Remove	You can use this button to delete selected permissions (see Deleting business role entitlements on page 624)(see Deleting department entitlements on page 598)(see Deleting cost center entitlements on page 667)(see Deleting entitlements from locations on page 723). To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 908: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – Location (page description)

To open the **Compliance - Location** page go to **Responsibilities** > **Governance Administration** > **Locations** > **Edit** > **Compliance**.

On the **Compliance - Location** page, you can view compliance rule violations caused by the location (see Displaying location rule violations on page 724).

The following table gives an overview of the different content on the **Compliance – Location** page.

Table 909: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – Location (page description)

To open the **Attestation - Location** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Attestation**.

On the **Attestation - Location** page you can:

- Display all attestation cases linked to this location (see Displaying location attestation cases on page 727)
- Display details of the objects being attested (see Displaying location attestation cases on page 727)
- Make approval decisions about pending attestation cases (see Approving and denying location attestation cases on page 730)
- Display attestors of pending attestation cases (see Displaying attestors of location pending attestation cases on page 729)
- Send reminders to approvers (see Sending reminders about location pending attestation cases on page 731)

The following tables give you overview of the various features and contents of the **Attestation – Location** page.

Table 910: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about location pending attestation cases on page 731).
Approve	Opens the **Pending Attestations – Locations** (see Pending attestations – Location (page description) on page 916). Use this button to make approval decisions about attestation cases pending for the location (see Approving and denying location attestation cases on page 730).

Table 911: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case Then you can send reminder emails to these identities (see Sending reminders about location pending attestation cases on page 731).
Show details	You can use this button to display details about all the objects that are included in this attestation case

Table 912: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – Location (page description)

To open the **Risk – Location** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Risk**.

On the **Risk – Location** page, you can:

- Display the location's calculated risk index (see Displaying location risk indexes on page 733)
- Show how the calculated risk index is put together

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the various features and content on the **Risk – Location** page.

Table 913: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index.

Table 914: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – Location (page description)

To open the **History - Location** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **History**.

On the **History – Location** page, you can see all the changes made to the location (see Location history on page 734).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows you all the events, which affect a location, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.
- **Status overview**: Shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – Location** page.

Table 915: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Disable this check box if you also want to see properties that have not changed since they were created.

Table 916: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 917: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	

Column	Description
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Location (page description)

To open the **Usage - Location** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Usage**.

On the **Usage - Location** page, you can see which roles the location members belong to (see Displaying role memberships of location members on page 737).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the different functions on the **Usage – Location** page.

Table 918: Controls

Control	Description
Role classes	You can select the main category of roles and organizations you want to display from this menu.
More information	Use this button to show the legend that explains the content of the overview.

Compliance reports - Location (page description)

To open the **Compliance Reports – Location** page go to **Responsibilities** > **Governance Administration** > **Organization** > **Edit** > **Compliance Reports**.

On the **Compliance Reports – Location** page you can:

- Display the location's policy violations (see Displaying location policy violations on page 725)
- Display rule violations of location members (see Displaying rule violations of location members on page 725)
- Display risk indexes and entitlements of location members (see Displaying risk indexes and entitlements of location members on page 726)

The information is divided into three parts:

- **Policy violations**: Shows all the current policy violations caused by the location.
- **Compliance rule violations**: Shows you all current rule violations of the identities assigned to the location.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and entitlements**: Shows all identities assigned to the location. In addition, the number of entitlements and risk index assigned to these identities is displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – Location** page.

Table 919: Columns

Column	Description
Policy violations	
Violating object	Show which object caused the rule violation.
Policy	Show the policy that was violated.
Status	Show the status of the rule policy.
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows the violated rule.
Approval state	Shows how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied.

Column	Description
	Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.
Identities: Risk index and entitlements	
Identity	Shows you the identity to which this location is assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Resources (page description)

To open the **Resources** page go to **Responsibilities** > **Governance Administration** > **Resources**.

On the **Resources** page you can see all resources (see Displaying all resources on page 705).

If you click **Edit** in a resource's details pane, a new page opens, which contains more information and configuration options for the resource (see Resource (page description) on page 1444).

The following table gives you an overview of the various content of the **Resources** page.

Table 920: Columns

Column	Description
Display	Shows you the resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Resource (page description)

To open the **Resource** page go to **Responsibilities** > **Governance Administration** > **Resources** > **Edit**.

On the **Resource** page, you can perform various actions on the resource you selected beforehand.

To do this, click on one of the tiles:

Table 921: Tiles

Tiles	Description
Overview	Opens the **Overview - Resource** page (see Overview – Resource (page description) on page 1446). This provides you with all the information at a glance (see Displaying resource overviews on page 706). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Resource** page (see Main data – Resource (page description) on page 1446). Here you can display and edit the resource's main data (see Displaying and editing resource main data on page 706).
Memberships	Opens the **Memberships - Resource** page (see Memberships – Resource (page description) on page 1447). You select the following actions: • Display identities that are assigned this resource (see Displaying resource memberships on page 707) • Request the resource for identities (see Assigning identities to resources on page 707) • Cancel this resource for identities (see Removing resources from identities on page 708)
Attestation	Opens the **Attestation – Resource** page (see Attestation - Resource (page description) on page 1448). You select the following actions: • Display all attestation cases linked to this resource (see Displaying resource attestation cases on page 709) • Display details of the objects being attested (see Displaying resource attestation cases on page 709) • Make approval decisions about pending attestation cases (see Approving and denying resource attestation cases on page 712) • Display attestors of pending attestation cases (see Displaying attestors of resource pending attestation cases on page 711) • Send reminders to approvers (see Sending reminders about resource pending attestation cases on page 713)
Usage	Opens the **Usage – Resource** page (see Usage – Resource (page description) on page 1450). Here you can display which roles the members of the resource belong to (see Displaying role memberships resource members on page 715).

Overview – Resource (page description)

To open the **Overview - Resource** page go to **Responsibilities** > **Governance Administration** > **Resources** > **Edit** > **Overview**.

On the **Overview – Resource** page, you can see all the information relevant to the resource summarized in an overview (see Displaying resource overviews on page 706).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Resource (page description)

To open the **Main data - Resource** page go to **Responsibilities** > **Governance Administration** > **Resources** > **Edit** > **Main data**.

On the **Main data - Resource** page, you can show and edit the resource's main data (see Displaying and editing resource main data on page 706).

The following tables give you an overview of the different functions and content on the **Main data – Resource** page.

Table 922: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 923: Resource main data

Property	Description
Resource	Enter a full, descriptive name for the resource.
Resource type	Select a resource type for the resource. Use resource types to group resources.
Description	Enter a description for the resource.
IT shop	Select the check box if the resource can also be requested through the IT Shop. The resource can be requested by identities through the Web Portal and the request granted by a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the resource can only be requested through the IT Shop. The resource can be requested by identities through the Web Portal and the request granted by a defined approval process. It is not possible to assign the resource directly to roles outside the IT Shop (for example, in Manager).
Service item	Click **Create a new service item** and create a new service item (a

Property	Description
	product). If a service item is already assigned, click **Change** and select a service item. You cannot use an assignment resource until a service item has been assigned to it.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning resources to identities. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Memberships – Resource (page description)

To open the **Memberships – Resource** page go to **Responsibilities** > **Governance Administration** > **Resources** > **Edit** > **Memberships**.

On the **Memberships – Resource** page, you can:

- Display identities that are assigned this resource (see Displaying resource memberships on page 707)
- Request the resource for identities (see Assigning identities to resources on page 707)
- Cancel this resource for identities (see Removing resources from identities on page 708)

The following tables give you an overview of the different functions and content on the **Memberships – Resource** page.

Table 924: Controls

Control	Description
Request memberships	Use this button to request the resource for identities (see Assigning identities to resources on page 707).
Delete member-ships	You can use this button to delete the resource assignment for selected identities (see Removing resources from identities on page 708). Select the check boxes in front of the identities whose resource assign-ments you want to delete and click this button.

Table 925: Columns

Column	Description
Identity	Shows you the name of the identity to which the resource is assigned.
Origin	Shows you whether the resource was assigned to the identity directly or indir-ectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation - Resource (page description)

To open the **Attestation - Resource** page go to **Responsibilities** > **Governance Administration** > **Resources** > **Edit** > **Attestation**.

On the **Attestation - Resource** page you can:

- Display all attestation cases linked to this resource (see Displaying resource attestation cases on page 709)
- Display details of the objects being attested (see Displaying resource attestation cases on page 709)
- Make approval decisions about pending attestation cases (see Approving and denying resource attestation cases on page 712)
- Display attestors of pending attestation cases (see Displaying attestors of resource pending attestation cases on page 711)
- Send reminders to approvers (see Sending reminders about resource pending attestation cases on page 713)

The following tables give you an overview of the various features and contents of the **Attestation – Resource** page.

Table 926: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about resource pending attestation cases on page 713).

Control	Description
Approve	Opens the **Pending Attestations – Resources** (see Pending attestations – Resource (page description) on page 947). Use this button to make approval decisions about attestation cases pending for the resource (see Approving and denying resource attestation cases on page 712).

Table 927: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case Then you can send reminder emails to these identities (see Sending reminders about resource pending attestation cases on page 713).
Show details	You can use this button to display details about all the objects that are included in this attestation case

Table 928: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – Resource (page description)

To open the **Usage - Resource** page go to **Responsibilities** > **Governance Administration** > **Resources** > **Edit** > **Usage**.

On the **Usage - Resource** page, you can see which roles the resource members belong to (see Displaying role memberships resource members on page 715).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following table gives you an overview of the various features on the **Usage – Resources** page.

Table 929: Controls

Control	Description
Role classes	You can select the main category of roles and organizations you want to display from this menu.
More information	Use this button to show the legend that explains the content of the overview.

System entitlements (page description)

To open the **System Entitlements** page go to **Responsibilities** > **Governance Administration** > **System Entitlements**.

On the **System entitlements** page, you can see all system entitlements (see Displaying all system entitlements on page 742).

If you click a system entitlement in the list, a new page opens, which contains more information and configuration options for the system entitlement (see System entitlement (page description) on page 1451).

The following table gives you an overview of the various features on the **System Entitlements** page.

Table 930: Columns

Column	Description
System entitlement	Shows the system entitlement's name.
Container	Shows you the container that holds the system entitlement.
Target system	Shows you to which target system the system entitlement belongs.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

System entitlement (page description)

To open the **System entitlement** page go to **Responsibilities** > **Governance Administration** > **System Entitlements** > click a system entitlement.

On the **System entitlement** page, you can perform various actions on the system entitlement you selected beforehand.

To do this, click on one of the tiles:

Table 931: Tiles

Tiles	Description
Overview	Opens the **Overview - System entitlement** page (see Overview – System entitlement (page description) on page 1453). This provides you with all the information at a glance (see Displaying system entitlement overviews on page 742). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - System entitlement** page (see Main data – System entitlement (page description) on page 1453). Here you can view and edit the system entitlement's main data (see Displaying and editing system entitlements main data on page 743).
Memberships	Opens the **Memberships - System entitlement** page (see Memberships – System entitlement (page description) on page 1455). You select the following actions: • Display identities that are assigned this system entitlement (see Displaying system entitlement memberships on page 745) • Request this system entitlement for identities (see Assigning identity system entitlements on page 745) • Cancel this system entitlement for identities (see Removing system entitlements from identities on page 746)
Attestation	Opens the **Attestations – System entitlement** page (see Attestation – System entitlement (page description) on page 1457). You select the following actions: • Display all attestation cases linked to this system entitlement (see Displaying system entitlement attestation cases on page 749) • Display details of the objects being attested (see Displaying system entitlement attestation cases on page 749) • Make approval decisions about pending attestation cases (see Approving and denying system entitlement attestation cases on page 751) • Display attestors of pending attestation cases (see Displaying attestors of system entitlement pending attestation cases on page

Tiles	Description
	750) • Send reminders to approvers (see Sending reminders about system entitlement pending attestation cases on page 753)
Attestors	Opens the **Attestors – System entitlement** page (see Attestors – System entitlement (page description) on page 1459). You select the following actions: • Display all identities that can approve the system entitlement's attestation cases (see Displaying system entitlement attestors on page 755) • Specify attestors for the system entitlement (see Specifying attestors of system entitlements on page 755) • Create new application roles for attestors (see Specifying attestors of system entitlements on page 755)
Child groups	Open the **Child groups – System entitlement** (see Child groups – System entitlement (page description) on page 1456). You select the following actions: • Display all the system entitlement's child groups (see Displaying system entitlements' child groups on page 747) • Assign a child group to the system entitlement (see Assigning child groups to system entitlements on page 748) • Remove child groups from the system entitlement (see Removing system entitlements' child groups on page 748)
Owner	Opens the **Owners – System entitlement** page (see Owners – System entitlement (page description) on page 1459). You select the following actions: • Show all the identities that are owners of the system entitlement (see Displaying product owners of system entitlements on page 757) • Specify owners of the system entitlement (see Specifying product owners for system entitlements on page 757) • Create new application roles for owners (see Specifying product owners for system entitlements on page 757)
History	Opens the **History – System entitlement** page (see History – System entitlement (page description) on page 1460). Here you can view all changes to the system authorization (see System entitlement history on page 759).

Tiles	Description
Usage	Opens the **Usage – System entitlement** page (see Usage – System entitlement (page description) on page 1463). Here you see which roles belong to the members of the system entitlement (see Displaying role memberships of system entitlement members on page 762).

Overview – System entitlement (page description)

To open the **Overview - System entitlement** page go to **Responsibilities** > **Governance Administration** > **System Entitlements**> click a system entitlement > **Overview**.

On the **Overview – System entitlement** page, you can display all the information relevant to the system entitlement summarized in an overview (see Displaying system entitlement overviews on page 742).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – System entitlement (page description)

To open the **Main data - System Entitlement** page go to **Responsibilities** > **Governance Administration** > **System Entitlements** > click a system entitlement > **Main data**.

On the **Main data - System entitlement** page, you can show and edit the system entitlement's main data (see Displaying and editing system entitlements main data on page 743).

The following table gives you an overview of the various features and content on the **Main data – System entitlement** page.

Table 932: Controls

Control	Description
Request modification	NOTE: This button is only available for Active Directory groups. Use this button to request the changes to the following properties of the Active Directory group (see Displaying and editing system entitlements main data on page 743): • **Group scope**: Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can specify one of the following group scopes: ◦ **Global group**: Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group’s domain.

Control	Description
	• **Local**: Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain. • **Universal**: Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure. • **Group type**: Specify whether this is an Active Directory security group or an Active Directory distribution group.
Request deletion	NOTE: This button is only available for Active Directory groups. Use this button to request to delete the group (see Deleting Active Directory groups on page 744).
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 933: System entitlement main data

Property	Description
Name	Enter a full, descriptive name for the system entitlement.
Canonical name	Shows the automatically generated canonical name of the system entitlement.
Distinguished name	Shows the automatically generated distinguished name of the system entitlement.
Display name	Enter a name for displaying the system entitlement in the One Identity Manager tools.
Notes domain	Shows the Notes domain name.
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use a system entitlement until a service item has been assigned to it.
Description	Enter a description for the system entitlement.
Category	Select the category for system entitlement inheritance. User accounts can inherit system entitlements selectively. To do this, system entitlements and user accounts are divided into categories.

Property	Description
Risk index	Use the slider to define the risk index. This value is used to assess the risk of assigning system entitlements to user accounts. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
IT shop	Enable this check box to allow the system entitlement to be requested through the IT Shop. This system entitlement can be requested by your identities through the Web Portal and granted through a defined approval process. The system entitlement can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Enable the check box to allow the system entitlement to be requested through the IT Shop if required. This system entitlement can be requested by your identities through the Web Portal and granted using a defined approval process. The system entitlement may not be assigned directly to hierarchical roles.
IT shop product is inactive	Select the check box if the system entitlement is not used. Only enabled system entitlements can be assigned within One Identity Manager. If a system entitlement is disabled, assignment of the system entitlement is not permitted. However, existing assignments remain intact.

Memberships – System entitlement (page description)

To open the **Memberships – System entitlement** page go to **Responsibilities** > **Governance Administration** > **System Entitlements** > select system entitlement > **Memberships**.

On the **Memberships – System entitlement** page, you can:

- Display identities that are assigned this system entitlement (see Displaying system entitlement memberships on page 745)
- Request this system entitlement for identities (see Assigning identity system entitlements on page 745)
- Cancel this system entitlement for identities (see Removing system entitlements from identities on page 746)

The following tables give you an overview of the different functions and content on the **Memberships – System entitlement** page.

Table 934: Controls

Control	Description
Request memberships	Use this button to request the system entitlement for identities (see Assigning identity system entitlements on page 745).
Delete member-	Use this button to delete membership of selected identities in the

Control	Description
ships	system entitlement (see Removing system entitlements from identities on page 746). Select the check box in front of the identities whose membership in the system entitlement you want to delete and click this button.

Table 935: Columns

Column	Description
Identity	Shows you the name of the identity to which the system entitlement is assigned.
Origin	Shows you whether the system entitlement was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Child groups – System entitlement (page description)

To open the **Child groups – system entitlement** page go to **Responsibilities** > **Governance Administration** > **System entitlements** > click system entitlement > **Child groups**.

On the **Child groups – System entitlement** page, you can:

- Display all the system entitlement's child groups (see Displaying system entitlements' child groups on page 747)
- Assign a child group to the system entitlement (see Assigning child groups to system entitlements on page 748)
- Remove child groups from the system entitlement (see Removing system entitlements' child groups on page 748)

The following table gives you an overview of the different features and content on the **Child groups – System entitlement** page.

Table 936: Controls

Control	Description
Remove selected	Use this button to remove selected child groups (see Removing system entitlements' child groups on page 748). Select the check box in front of the group that you want to remove and click this button.
New child group	Use this button to assign a child group to the system entitlement (see Assigning child groups to system entitlements on page 748).

Attestation – System entitlement (page description)

To open the **Attestation - System Entitlements** page go to **Responsibilities** > **Governance Administration** > **System Entitlements** > click a system entitlement > **Attestation**.

On the **Attestation - System entitlement** page you can:

- Display all attestation cases linked to this system entitlement (see Displaying system entitlement attestation cases on page 749)
- Display details of the objects being attested (see Displaying system entitlement attestation cases on page 749)
- Make approval decisions about pending attestation cases (see Approving and denying system entitlement attestation cases on page 751)
- Display attestors of pending attestation cases (see Displaying attestors of system entitlement pending attestation cases on page 750)
- Send reminders to approvers (see Sending reminders about system entitlement pending attestation cases on page 753)

The following tables give you overview of the various features and contents of the **Attestation – System entitlement** page.

Table 937: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about system entitlement pending attestation cases on page 753).
Approve	Opens the **Pending Attestations – System entitlements** page (see Pending attestations – System entitlement (page description) on page 943).

Control	Description
	Use this button to make approval decisions about attestation cases pending for the system entitlement (see Approving and denying system entitlement attestation cases on page 751).

Table 938: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case Then you can send reminder emails to these identities (see Sending reminders about system entitlement pending attestation cases on page 753).
Show details	You can use this button to display details about all the objects that are included in this attestation case

Table 939: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestors – System entitlement (page description)

To open the **Attestors – system entitlement** page go to **Responsibilities** > **Governance Administration** > **System entitlements** > click system entitlement > **Attestors**.

On the **Attestors – System entitlement** page, you can:

- Display all identities that can approve the system entitlement's attestation cases (see Displaying system entitlement attestors on page 755)
- Specify attestors for the system entitlement (see Specifying attestors of system entitlements on page 755)
- Create new application roles for attestors (see Specifying attestors of system entitlements on page 755)

The following tables give you an overview of the various features and content on the **Attestor – System entitlement** page.

Table 940: Controls

Control	Description
Attestors	Click **Assign**/**Change** and select an application role whose members can approve the system entitlement's attestation cases. To save the changes, click **Save**. For more information, see Specifying attestors of system entitlements on page 755.
New	Use this button to create a new application role (see Specifying attestors of system entitlements on page 755). Then you can assign identities to the new application role that can approve the system entitlement's attestation cases. To save the changes, click **Save**.
Save	Use this button to save all the changes you have made.

Table 941: Columns

Column	Description
Name	Shows you the name of the identity that you can assign to the application role.
Primary department	Shows you which department is assigned as primary to the identity.
Identity	Shows you whether this is a main or a sub identity.

Owners – System entitlement (page description)

To open the **Owners – System entitlement** page go to **Responsibilities** > **Governance Administration** > **System entitlements** > click system entitlement > **Owner**.

On the **Owners – System entitlement** page, you can:

- Show all the identities that are owners of the system entitlement (see Displaying product owners of system entitlements on page 757)
- Specify owners of the system entitlement (see Specifying product owners for system entitlements on page 757)
- Create new application roles for owners (see Specifying product owners for system entitlements on page 757)

The following tables give you an overview of the different features and content on the **Owners – System entitlement** page.

Table 942: Controls

Control	Description
Product owners	Click **Assign**/**Change** and select an application role whose members will be owners of the system entitlement. To save the changes, click **Save**. For more information, see Specifying product owners for system entitlements on page 757.
New	Use this button to create a new application role (see Specifying product owners for system entitlements on page 757). Then you can assign identities to the new application role to be the owners of the system entitlement. To save the changes, click **Save**.
Move ownership	Use this button to create a new application role and, at the same time, transfer all the currently assigned owners to it. To save the changes, click **Save**. For more information, see Specifying product owners for system entitlements on page 757.
Save	Use this button to save all the changes you have made.

Table 943: Columns

Column	Description
Name	Shows you the name of the identity that you can assign to the application role.
Primary department	Shows you which department is assigned as primary to the identity.
Identity	Shows you whether this is a main or a sub identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

History – System entitlement (page description)

To open the **History - System Entitlement** page go to **Responsibilities** > **Governance Administration** > **System Entitlements** > click a system entitlement > **History**.

On the **History – System entitlements** page, you can see all the changes made to the system entitlement (see System entitlement history on page 759).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows you all the events that affect a system entitlement, either on a timeline or in a table.

  TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

  To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – System entitlement** page.

Table 944: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Disable this check box if you also want to see properties that have not changed since they were created.

Table 945: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the

Control	Description
	selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 946: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – System entitlement (page description)

To open the **Usage – System entitlement** page go to **Responsibilities** > **Governance Administration** > **System Entitlements** > select system entitlement > **Usage**.

On the **Usage - System entitlement** page, you can see which roles the system entitlement members belong to (see Displaying role memberships of system entitlement members on page 762).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the different functions on the **Usage – System entitlement** page.

Table 947: Controls

Control	Description
Role classes	You can select the main category of roles and organizations you want to display from this menu.
More information	Use this button to show the legend that explains the content of the overview.

System roles (page description)

To open the **System Roles** page go to **Responsibilities** > **Governance Administration** > **System Roles**.

On the **System Roles** page, you can see all system roles (see Displaying all system roles on page 763).

If you click **Edit** in a system role's details pane, a new page opens, which contains more information and configuration options for the system role (see System role (page description) on page 1463).

The following table gives an overview of the various content of the **System role** page.

Table 948: Columns

Column	Description
Display	Shows you the system role's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

System role (page description)

To open the **System Role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit**.

On the **System role** page, you can perform various actions on the system role you selected beforehand.

To do this, click on one of the tiles:

Table 949: Tiles

Tiles	Description
Overview	Opens the **Overview - System role** page (see Overview – System role (page description) on page 1466). This provides you with all the information at a glance (see Displaying system role overviews on page 764). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - System role** page (see Main data – System role (page description) on page 1466). Here you can view and edit the system role's main data (see Displaying and editing system role main data on page 764).
Memberships	Opens the **Memberships - System role** page (see Memberships – System role (page description) on page 1467). You select the following actions: • Display identities that are assigned this system role (see Displaying system role memberships on page 765) • Request the system role for identities (see Assigning identities to system roles on page 766) • Cancel this system role for identities (see Removing identities from my system roles on page 766)
Permissions	Opens the **Entitlements – System role** page (see Entitlements – System role (page description) on page 1468). You select the following actions: • Display entitlements assigned to the system role (see Displaying system role entitlements on page 767) • Add new entitlements to the system role (see Adding system role entitlements on page 768) • Delete system role entitlements (see Deleting system role entitlements on page 769)
Compliance	Opens the **Compliance – System role** page (see Compliance – System role (page description) on page 1469). Here you can display compliance rule violations caused by the system role (seeDisplaying system role rule violations on page 770).
Attestation	Opens the **Attestation – System role** page (see Attestation – System role (page description) on page 1470).

Tiles	Description
	You select the following actions: • Display all attestation cases linked to this system role (see Displaying system role attestation cases on page 773) • Display details of the objects being attested (see Displaying system role attestation cases on page 773) • Make approval decisions about pending attestation cases (see Approving and denying system role attestation cases on page 775) • Display attestors of pending attestation cases (see Displaying attestors of system role pending attestation cases on page 774) • Send reminders to approvers (see Sending reminders about system role pending attestation cases on page 776)
Risk	Opens the **Risk – System role** page (see Risk – System role (page description) on page 1472). You select the following actions: • Display the system role's calculated risk index (see Displaying system role risk indexes on page 778) • Show how the calculated risk index is put together
History	Opens the **History – System role** page (see History – System role (page description) on page 1472). Here you can view all changes made to the system role (see System role history on page 779).
Usage	Opens the **Usage – System role** page (see Usage – System role (page description) on page 1474). Here you can display which roles the members of the system role belong to (see Displaying role memberships of system role members on page 782).
Compliance reports	Opens the **Compliance report – System role** page (see Compliance reports – system role (page description) on page 1475). You select the following actions: • Display the system role's policy violations (see Displaying system role policy violations on page 771) • Display rule violations of system role members (see Displaying rule violations of system role members on page 771) • Display risk indexes and entitlements of system role members (see Displaying risk indexes and entitlements of system role members on page 772)

Overview – System role (page description)

To open the **Overview - System Role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit> Overview**.

On the **Overview - System role** page, you can display all relevant information about the system role in summarized in an overview (see Displaying system role overviews on page 764).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – System role (page description)

To open the **Main data – System role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit**> **Main data**.

On the **Main data - System role** page, you can show and edit the system role's main data (see Displaying and editing system role main data on page 764).

The following tables give you an overview of the different functions and content on the **Main data – System role** page.

Table 950: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 951: System role main data

Property	Description
System role	Enter a full, descriptive name for the system role.
Display name	Enter a name for displaying the system role in the One Identity Manager tools.
Internal product name	Enter a company internal name for the system role.
System role type	Select the role type of the system role. The system role type specifies which type of company resources make up the system role.
Service item	Click **Create a new service item** and create a new service item (a product). If a service item is already assigned, click **Change** and select a service item. You cannot use a system role until a service item has been assigned to

Property	Description
	it.
System role manager	Click **Change** and select the identity responsible for the system role. This identity can edit the system role's main data and be used as an attestor for system role properties. If the system role can be requested in the IT Shop, the manager will automatically be a member of the application role for product owners assigned the service item.
Comment	Enter a comment for the system role.
IT shop	Select the check box if the system role can also be requested through the IT Shop. This system role can be requested by identities through the Web Portal and the request granted by a defined approval process. The system role can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*.
Only use in IT Shop	Select the check box if the system role can only be requested through the IT Shop. This system role can be requested by identities through the Web Portal and the request granted by a defined approval process. The system role may not be assigned directly to hierarchical roles.

Memberships – System role (page description)

To open the **Memberships – System Role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit** > **Memberships**.

On the **Memberships – System role** page, you can:

- Display identities that are assigned this system role (see Displaying system role memberships on page 765)
- Request the system role for identities (see Assigning identities to system roles on page 766)
- Cancel this system role for identities (see Removing identities from my system roles on page 766)

The following tables give you an overview of the different functions and content on the **Memberships – System role** page.

Table 952: Controls

Control	Description
Request memberships	Use this button to request the system role for identities (see Assigning identities to system roles on page 766).
Delete member-ships	Use this button to delete membership of selected identities in the system role (see Removing identities from my system roles on page

Control	Description
	766). Select the check box in front of the identities whose membership in the system role you want to delete and click this button.

Table 953: Columns

Column	Description
Identity	Shows you the name of the identity to which the system role is assigned.
Origin	Shows you whether the system role was assigned to the identity directly or indirectly.

TIP: For each identity, you can see more useful information in the details pane. To do this, click the appropriate instance in the list. If the identity did not receive the membership through a direct assignment (for example, through an assignment request or delegation), the **Request** tab provides more information:

- **Information**: Displays general information about a request. The information displayed varies and is dependent on the service category from which the request was triggered.
- **Workflow**: Displays the life cycle chronologically as from the time of request.
- **Compliance**: Displays possible rule violations for this request.
- **Entitlements**: Show which entitlement are assigned to the role (if a role was requested).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Entitlements – System role (page description)

To open the **Entitlements - System Role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit** > **Entitlements**.

On the **Entitlements – System role** page, you can:

- Display entitlements assigned to the system role (see Displaying system role entitlements on page 767)
- Add new entitlements to the system role (see Adding system role entitlements on page 768)
- Delete system role entitlements (see Deleting system role entitlements on page 769)

TIP: Entitlements form the basis for membership in an object (for example in a department).

The following tables give you an overview of the various features and content on the **Entitlements – System role** page.

Table 954: Controls

Control	Description
New	
Remove	You can use this button to delete selected permissions (see Deleting business role entitlements on page 624)(see Deleting department entitlements on page 598)(see Deleting cost center entitlements on page 667)(see Deleting entitlements from locations on page 723). To do this, select the check box in front of the entitlement you want to delete and click the button.

Table 955: Columns

Column	Description
Entitlement	Shows you the entitlement's name.
Origin	Shows you how the entitlement was assigned. For example, the entitlement might have been assigned through a dynamic role.
Entitlement type	Shows you the entitlement type (for example, report subscriptions, account definition, resources).

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Compliance – System role (page description)

To open the **Compliance - System Role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit** > **Compliance**.

On the **Compliance - System Role** page, you can view compliance rule violations caused by the system role (seeDisplaying system role rule violations on page 770).

The following table gives an overview of the content of the **Compliance – System role** page.

Table 956: Columns

Column	Description
Entitlement	Shows the entitlement that caused the rule violation.
Rule	Shows the rule that was violated.
Risk index	Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk that this rule violation poses.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied.

Column	Description
	Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.

TIP: On the following tabs, you can show other useful information about each rule violation in the pane. To do this, click the corresponding entry in the list.

- **Entitlement**: Shows general information about the entitlement.
- **Rule**: Show general information about rule that was violated.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Attestation – System role (page description)

To open the **Attestation - System Role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit** > **Attestation**.

On the **Attestation - System Role** page you can:

- Display all attestation cases linked to this system role (see Displaying system role attestation cases on page 773)
- Display details of the objects being attested (see Displaying system role attestation cases on page 773)
- Make approval decisions about pending attestation cases (see Approving and denying system role attestation cases on page 775)
- Display attestors of pending attestation cases (see Displaying attestors of system role pending attestation cases on page 774)
- Send reminders to approvers (see Sending reminders about system role pending attestation cases on page 776)

The following tables give you overview of the various features and contents of the **Attestation – System Role** page.

Table 957: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases Then you can send them reminder mails.
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about system role pending attestation cases on page 776).
Approve	Opens the **Pending Attestations – System roles** (see Pending attestations – System role (page description) on page 912).

Control	Description
	Use this button to make approval decisions about attestation cases pending for the system role (see Approving and denying system role attestation cases on page 775).

Table 958: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case Then you can send reminder emails to these identities (see Sending reminders about system role pending attestation cases on page 776).
Show details	You can use this button to display details about all the objects that are included in this attestation case

Table 959: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Risk – System role (page description)

To open the **Risk – System role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit** > **Risk**.

On the **Risk – System role** page, you can:

- Display the system role's calculated risk index (see Displaying system role risk indexes on page 778)
- Show how the calculated risk index is put together

The risk index is calculated from the sum of all attribute-based values and the maximum of all assignment-based values.

The following tables give you an overview of the various features and content on the **Risk – System role** page.

Table 960: Controls

Control	Description
View risk functions	Use this button to show the attributes and assignments that contribute to the calculated risk index.

Table 961: Columns

Column	Description
Risk index	Shows which property/assignment affects the risk index.
Risk	• At root level: Shows the summarized risk index of the property/assignment. • At other levels: Shows other details about the properties/assignments.
Weighting/change value	Shows, depending on the type of calculation, the value used to weigh the determined risk index in the overall calculation or the value used to alter the risk index respectively.

History – System role (page description)

To open the **History - System Role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit** > **History**.

On the **History – System role** page, you can see all the changes made to the system role (see System role history on page 779).

NOTE: Which changes are shown depends on your system's configuration.

The information is divided out on to three tabs:

- **Events**: Shows you all the events, which affect a system role, either on a timeline or in a table.

TIP: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.

To zoom in or out, turn the mouse wheel.

- **Status overview**: Shows you an overview of all assignments. It also shows how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.
- **Status comparison**: You can select a date and display all the changes made from then until now. You can also show what the value of the property was at the selected point in time and what the value is now.

The following tables give you an overview of the different functions and content on the **History – System role** page.

Table 962: Controls

Control	Description
Events tab	
Filter by	Use this function to filter the changes by a specific criteria. For example, you can just display changes from a certain user. TIP: To remove the filter again, click (**Reset filter**) next to the corresponding filter.
Switch to table view	Use this button to display the changes in table form.
Switch to timeline view	Use this button to display the changes as a timeline.
Status comparison tab	
Time and date picker	Select from which point on you want to see the changes.
Display changed values only	Disable this check box if you also want to see properties that have not changed since they were created.

Table 963: Controls in the details pane of a change

Control	Description
Compare	Opens the **Status comparison** tab. Use this button to show all the changes that were made from the selected point in time until now. You can also show what the value of the property was at the selected point in time and what the value is now.

Table 964: Columns

Column	Description
Events tab (table view)	
Change type	Shows the type of change.
Property	Shows the name of the property that was changed.
Display	Shows the value that was changed. For example, the name of a department.
Date	Shows the date the change was made.
User	Shows the user that made the change.
Status overview tab	
Display	Shows the type of change.
Property	Shows the name of the property that was changed.
Value	Shows the value that was changed. For example, the name of a department.
Run started	Shows when the change was made.
End	Shows for how long the changed value applied or whether it is currently in use.
Status comparison tab	
Modified	Show whether the change took place or not.
Change type	Shows the type of change.
Object type	Show the type of object involved in the change.
Property	Show the name of the object that was changed.
Historical value	Shows the value before the change was made.
Current value	Shows the value that is currently in use.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Usage – System role (page description)

To open the **Usage - System role** page, go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit** > **Usage**.

On the **Usage – System role** page, you can see which roles system role members belong to (see Displaying role memberships of system role members on page 782).

The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the different functions on the **Usage – System role** page.

Table 965: Controls

Control	Description
Role classes	You can select the main category of roles and organizations you want to display from this menu.
More information	Use this button to show the legend that explains the content of the overview.

Compliance reports – system role (page description)

To open the **Compliance Reports – System Role** page go to **Responsibilities** > **Governance Administration** > **System Roles** > **Edit** > **Compliance Reports**.

On the **Compliance Reports – System role** page you can:

- Display the system role's policy violations (see Displaying system role policy violations on page 771)
- Display rule violations of system role members (see Displaying rule violations of system role members on page 771)
- Display risk indexes and entitlements of system role members (see Displaying risk indexes and entitlements of system role members on page 772)

The information is divided into three parts:

- **Policy violations**: Shows all the current policy violations caused by the system role.
- **Compliance rule violations**: Shows you the current rule violations of the identities to which the system role is assigned.

  TIP: For more information about resolving rule violations, see Resolving rule violations on page 204.
- **Identities: Risk index and entitlements**: Displays all identities to which the system role is assigned. In addition, the number of entitlements and risk index assigned to these identities is displayed.

To display the information, select the item you want from the **View** menu.

The following table gives an overview of the content of the **Compliance reports – System role** page.

Table 966: Columns

Column	Description
Policy violations	
Violating object	Show which object caused the rule violation.

Column	Description
Policy	Show the policy that was violated.
Status	Show the status of the rule policy.
Compliance rule violations	
Employee	Shows you the identity that caused the rule violation.
Rule violation	Shows the violated rule.
Approval state	Shows how or whether approval is granted to the rule violation.
Risk index (reduced)	Shows the risk index taking mitigating controls into account. A rule's risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Compliance – Governance Administration on page 209.
Identities: Risk index and entitlements	
Identity	Shows you the identity to which this system role is assigned.
Risk index (calculated)	Shows you the identity's calculated risk index.
Assigned permissions	Shows you all the entitlements assigned to this identity.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Assignment resources (page description)

To open the **Assignment resources** page go to **Responsibilities** > **Governance Administration** > **Assignment resources**.

On the **Assignment resources** page, you can see all the assignment resources (see Displaying all assignment resources on page 783).

If you click **Edit** in an assignment resource's details pane, a new page opens, which contains more information and configuration options for the assignment resource (see Assignment resource (page description) on page 1477).

The following table gives you an overview of the various features and content on the **Assignment resources** page.

Table 967: Columns

Column	Description
Display	Shows you the assignment resource's name.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Assignment resource (page description)

To open the **Assignment resource** page go to **Responsibilities** > **Governance Administration** > **Assignment resources** > **Edit**.

On the **Assignment resource** page, you can perform various actions on the assignment resource you selected beforehand.

To do this, click on one of the tiles:

Table 968: Tiles

Tiles	Description
Overview	Opens the **Overview - Assignment resource** page (see Overview – Assignment resource (page description) on page 1477). This provides you with all the information at a glance (see Displaying assignment resource overviews on page 784). For more information, click on the links inside one of the shapes.
Main data	Opens the **Main data - Assignment resource** page (see Main data – Assignment resource (page description) on page 1478). Here you can view and edit the assignment resource's main data (see Managing assignment resources on page 783).
Attestation	Opens the **Attestation – Assignment resource** page (see Attestation - Assignment resource (page description) on page 1479). You select the following actions: • Display all attestation cases linked to this assignment resource (see Displaying assignment resource attestation cases on page 785) • Display details of the objects being attested (see Displaying assignment resource attestation cases on page 785) • Make approval decisions about pending attestation cases (see Approving and denying assignment resource attestation cases on page 788) • Display attestors of pending attestation cases (seeDisplaying attestors of assignment resource pending attestation cases on page 787) • Send reminders to approvers (see Sending reminders about assignment resource pending attestation cases on page 789)

Overview – Assignment resource (page description)

To open the **Overview – Assignment resource** page go to **Responsibilities** > **Governance Administration** > **Assignment resources** > **Edit** > **Overview**.

On the **Overview - Assignment resource** page, you can display all relevant information about the assignment resource summarized in an overview (see Displaying assignment resource overviews on page 784).

This information is displayed as shapes. For more information, click on the links inside one of the shapes.

Main data – Assignment resource (page description)

To open the **Main data - Assignment Resource** page go to **Responsibilities** > **Governance Administration** > **Assignment Resources** > **Edit** > **Main data**.

On the **Main data - Assignment resource** page, you can show and edit the assignment resource's main data (see Managing assignment resources on page 783).

The following tables give you an overview of the different functions and content on the **Main data – Assignment resource** page.

Table 969: Controls

Control	Description
Save	Use this button to save the changes to the main data.

You can change the following main data.

Table 970: Assignment resource main data

Property	Description
Assignment resource	Enter a full, descriptive name for the assignment resource.
Resource type	Select the resource type of the assignment resource. Use resource types to group assignment resources.
Description	Enter a full, descriptive name for the assignments resource.
IT shop	Shows whether the assignment resource can be requested through the IT Shop. The assignment resource can be requested by its identities through the Web Portal and distributed using a defined approval process. For more information about IT Shop, see the *One Identity Manager IT Shop Administration Guide*. This option cannot be disabled.
Only use in IT Shop	Shows whether the assignment resource can only be requested through the IT Shop. The assignment resource can be requested by its identities through the Web Portal and distributed using a defined approval process. You cannot assign an assignment resource to hierarchical roles directly. This option cannot be disabled.
Service item	Click **Create a new service item** and create a new service item (a

Property	Description
	product). If a service item is already assigned, click **Change** and select a service item. You cannot use an assignment resource until a service item has been assigned to it.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning assignment resources to identities. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
Requested assignments remain intact.	Select the check box to convert assignments to roles into direct assignments if the request recipient is removed from the customer node of the associated shop. The option can only be edited as long as there is a request has not been assigned with this assignment resource.

Attestation - Assignment resource (page description)

To open the **Attestation - Assignment resource** page go to **Responsibilities** > **Governance Administration** > **Assignment resources** > **Edit** > **Attestation**.

On the **Attestation - Assignment resource** page you can:

- Display all attestation cases linked to this assignment resource (see Displaying assignment resource attestation cases on page 785)
- Display details of the objects being attested (see Displaying assignment resource attestation cases on page 785)
- Make approval decisions about pending attestation cases (see Approving and denying assignment resource attestation cases on page 788)
- Display attestors of pending attestation cases (seeDisplaying attestors of assignment resource pending attestation cases on page 787)
- Send reminders to approvers (see Sending reminders about assignment resource pending attestation cases on page 789)

The following tables provide an overview of the various functions and contents of the **Attestation – Assignment Resource** page.

Table 971: Controls

Control	Description
View approvers for pending cases	Use this button to display all identities that still have to make approval decisions about attestation cases Then you can send them reminder mails.

Control	Description
Send reminder	You can use this button to send reminder mails to all identities that still have attestation cases to approve on the current tab (see Sending reminders about assignment resource pending attestation cases on page 789).
Approve	Opens the **Pending Attestations – Assignment resources** (see Pending attestations – Assignment resource (page description) on page 951). Use this button to make approval decisions about attestation cases pending for the assignment resource (see Approving and denying assignment resource attestation cases on page 788).

Table 972: Controls in the attestation case's details pane

Control	Description
Actions > Send a reminder mail	Use this action to display all identities that can make approval decisions about the attestation case Then you can send reminder emails to these identities (see Sending reminders about assignment resource pending attestation cases on page 789).
Show details	You can use this button to display details about all the objects that are included in this attestation case

Table 973: Columns

Column	Description
Display name	Shows the name of the object included in the attestation case.
Attestation policy	Shows the name of the attestation policy in use.
State	Shows the current status of the attestation case. The following status' are possible: • **Pending**: The attestation case is not closed yet and must still be approved. • **Approved**: The attestation case was approved. In the details pane, on the **Workflow** tab, you can see why the attestation case was granted approval. • **Denied**: The attestation case was denied. In the details pane, on the **Workflow** tab, you can see why the attestation case was denied approval.
New	Shows whether the attestation case is new. New cases have not been granted approval yet but might have been denied approval before.

Column	Description
Due date	Shows by when the attestation case must be completed.
Risk index	Show the attestation case's risk index.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

Calls (Menu description)

You can use items on the **Calls** menu to perform various actions surrounding calls and collect information. The following tables provide you with an overview of the menu items and actions that can be run here.

Table 974: Menu items

Menu	Menu item	Description
Calls		
	New Call	Here you can create new calls.
	Call history	Here you can display all the calls.

New call (page description)

To open the **New Call** page go to **Calls** > **New Call**.

On the **New Call** page, submit a new call.

To record issues that can have different causes, you can create calls. For example, a call can be added for an identity who reports a issue or for products with specific terms of contract. Even devices or the workdesk associated with the problematic device, can be included when adding a call.

You can enter the following information:

Table 975: Main data of a call

Property	Description
Description	Enter a detailed description of the issue.
Product	Select the product involved in this issue.
Severity	Select how serious the issue is.

Property	Description
Cost center	Click **Assign**/**Change** and then select a cost center.
Additional staff	Click **Assign**/**Change**, and then select an identity as an additional contact person.

Call history (page description)

To open the **Call History** page go to **Calls** > **Call History**.

On the **Call History** page, you can display and edit all existing calls and their details.

The following tables give you an overview of the various features and content on the **Call History** page.

Table 976: Controls

Control	Description
Display calls	This view allows you to control which calls are displayed: • **Calls submitted by you for yourself**: Select this check box to display calls that you submitted for yourself. • **Calls submitted by you for others**: Select this check box to display calls you submitted for other identities. • **Calls submitted for you by others**: Select this check box to display calls that other identities submitted for your. • **Closed calls**: Check this box to display calls that have already been closed.

Table 977: Controls in the details pane of a call

Control	Description
Main data tab	
Severity	Select how serious the issue is.
Description	Add or change the issue's description here if necessary.
Last action	Shows you a description of the last action taken for this call. You can edit this action description.
Product	Select the product involved in this issue.
Add a comment	Enter a comment about the call. For example, you can specify what actions will be taken to correct the issue.
Save	Use this button to save your changes to the call.

Control	Description
Attachments tab	
Choose file	Use this button to attach a file to this call (for example, a screenshot).
Delete	Use this button to delete the attachment from the corresponding row.

Table 978: Columns

Column	Description
Display	Shows you the call number and the creation date of the call.
Description	Shows you the description of the issue.
Call status	Shows you the call is progressing
Reported by	Shows you which identity submitted the call.

TIP: You can show less data by using the column filters. For more information, see Filtering on page 40.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

B

C

D

K

L

M

N

O

P

T

U

V

W