ONE IDENTITY

by Quest

One Identity Manager 9.1

Web Portal User Guide

Contents

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.
- 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:
    - Firefox (release channel)
    - Chrome (release channel)
    - Safari (current version)
    - Microsoft Edge (release channel)

Detailed information about this topic

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

- Logging in on page 16
- Logging in to the Password Reset Portal on page 17
- Logging off on page 18

Logging in

Open the Web Portal in a web browser.

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 **User name** field, enter your full user name.

3. In the **Password** field, enter your personal password.

4. Click **Log in**.

Related topics

- Changing passwords on page 27

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, and manage your password questions.

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. Open the Password Reset Portal URL in your web browser.

   The Password Reset Portal opens.

2. On the login page, in the **Authentication** menu, select the **Login with passcode** option.

3. In the **User name** field, enter your user name.

4. In the **Enter characters from the image** field, enter the Captcha Code displayed.

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

5. Click **Next**.

6. In the **Passcode** field, enter your passcode.

7. Click **Submit**.

To log in to Password Reset Portal using your password questions

1. Open the Password Reset Portal URL in your web browser.

   The Password Reset Portal opens.

2. On the login page, in the **Authentication** menu, select the **Log in by answering your password questions** option.

3. In the **User name** field, enter your user name.

4. In the **Enter characters from the image** field, enter the Captcha Code displayed.

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

5. Click **Next**.

6. In the fields, enter the appropriate answers to your password questions.

7. Click **Submit**.

To log in to Password Reset Portal using your current password

1. Open the Password Reset Portal URL in your web browser.

   The Password Reset Portal opens.

2. On the login page, in the **Authentication** menu, select the corresponding authentication method.

3. In the **User name** field, enter your user name.

4. In the **Password** field, enter your personal password.

5. Click **Log in**.

Related topics

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 **Yes**.

   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

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.

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.
	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.

Example	Description
	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

Context searching

The context search is available to you where multiple items are listed.

To run a context search

1. In the 🔍 **Search** field, enter the search term.

   Any results matching your query are displayed.

2. (Optional) To clear the search, click ✖ (**Reset filter**).

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

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**) > .

Filtering

You can find the filter function represented by ▼ (**Filter**) on a lot of pages. It provides you with a selection of different filters.

| NOTE: The contents of the filters vary depending on context.

To use a filter

1. On the page with the filter function, click ▼ (**Filter**).

2. In the menu, enable the filter that you want to apply.

3. (Optional) To reset the filter, click ▼ (**Filter**) and then **Clear filters**.

Detailed information about this topic

- Custom filter conditions

Custom filter conditions

In some places in the Web Portal you can create custom filter conditions.

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

To use the wizard, first select a property then specify a comparison operator and a comparison value.

Comparison operators

You can use the following operators to define a condition. The type of comparison operator depends on the selected property.

Table 6: 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 include one of the given text values. Click **Add new value** to add another value.
	contains	Finds all results that contain the text value.
	starts 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.

Value type	Operator	Description
Date value	older than	Finds all results that are older than the given date.
	younger than	Finds all results that are younger than the given date.
	is equal to	Finds all results that are the same as the given date.
	older than or equal to	Finds all results that are greater than or equal to the given date.
	younger than or equal to	Finds all results that are younger than or equal to the given date.
	is not equal to	Finds all results that are not the same as the given date.
Boolean value	Property is activated	If the switch is set, all results are searched for where this property is enabled.
		If the switch is not set, all results are searched for where this property is disabled.

Comparison values

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

You can enter date values as relative (in hours, days, months, or years) but also as absolute values (fixed date).

Boolean values

Set the switch to display all data sets with this property is enabled.

Do not set the switch to display all data sets with this property is disabled.

Link conditions

To link conditions you can use the logical operators AND and OR.

Displaying the address book

If you need information about an identity such as the phone number or location, you can use the address book.

To display the address book

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

   This displays the address book and all identities.

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

   In the **Edit Identity Data** pane, there are further details about the identity.

Managing password questions

If you forget your password, you can change it at any time in the Web Portal (see Changing passwords on page 27). 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 25
- Editing password questions on page 26
- Deleting password questions on page 26

Creating password questions

You can create new password questions.

To create new a password question

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

2. On the **Profile Settings** page click the **Password Questions** tab.

3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.

4. On the **Password Questions** tab, click **Create password question**.

5. In the **Create Password Question** pane, enter the following:

   - **Question**: Enter your question.

   - **Answer**: Enter the answer to your question (above).

- **Repeat answer**: Enter the answer to your question again.

6. Click **Save**.

Editing password questions

You can edit existing password questions.

To edit a password question

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

2. On the **Profile Settings** page click the **Password Questions** tab.

3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.

4. In the **Password Questions** tab, click the password question you want to edit.

5. Click **Edit**.

6. Specify the following:

   - **Question**: Enter your question.

   - **Answer**: Enter the answer to your question (above).

   - **Repeat answer**: Enter the answer to your question again.

7. Click **Save**.

Deleting password questions

You can delete existing password questions.

To delete a password question

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

2. On the **Profile Settings** page click the **Password Questions** tab.

3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.

4. On the **Password Questions** tab, click the password question you want to delete.

5. Click **Delete**.

6. In the **Delete password question** dialog, confirm the prompt with **Yes**.

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 17).

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 27), 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 home page, in the **Passwords** tile, click **Manage passwords**.
2. On the **Manage My Passwords** page, click **Set new password** next to the user account you want to give a new password to.
3. In the **Set New Password** pane, in the **New password** field, enter the password you wish to use.
4. In the **Repeat the password** field, enter the password again.
5. Click **Save**.

To change the central password

1. On the home page, in the **Passwords** tile, click **Manage passwords**.
2. On the **Manage My Passwords** page, next to **Central password**, click **Set new password**.
3. In the **Set New Password** pane, in the **New password** field, enter the password you wish to use.
4. In the **Repeat the password** field, enter the password again.
5. Click **Save**.

   The central password is reset.

Related topics

- Managing password questions on page 25

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**) > **Profile**.
2. On the **Profile Settings** page, click the **Password Questions** tab.
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 **Add**/**Change**.
    b. Select an image from your medium.
6. Click **Save**.

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**) > **Profile**.
2. On the **Profile Settings** page, click the **Password Questions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. In the **Language** menu, select the language that you want to use for the Web Portal.
5. In the **Language for value formatting** menu, 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**).

6. Click **Save**.

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 header, click 👤 (**Profile**) > **My profile**.

2. On the **Profile 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 next to the event that you want to notified about.

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

5. 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

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 header, click 👤 (**Profile**) > **My profile**.

2. On the **Profile Settings** page, click the **Report Subscriptions** tab.

3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.

4. On the **Report Subscriptions** tab, click **Add subscription**.

   On the **Report Subscriptions** page, click **Add subscription**.

5. In the **Add Report Subscription** pane, in the list, click the report that you want to subscribe to.

   TIP: To search for a specific report, in the **Search** field, enter the name of the report.

6. Click **Next**.

7. In the **Configure subscription** 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.

   - **Parameter**: (Optional) Specify other report specific settings. These settings might vary depending on what report you use.

8. Click **Next**.

9. In the **Add additional subscribers** step, in the **Additional subscribers** list, click the identities that will also receive this report.

   TIP: To search for a specific identity, in the **Search** field, enter the name of the identity.

   TIP: To remove a subscriber, in the **Selected subscribers** list, click ✕ (**Remove**) next to the corresponding identity. To remove all subscribers, in the **Selected subscribers** list, click **Remove all**.

10. Click **Next**.

11. In the **Check and create subscription** step, check your data and change them if necessary by clicking on the respective step.

12. Click **Create**.

Editing report subscriptions

You can edit your existing report subscriptions.

To edit a report subscription

1. In the header, click 👤 (**Profile**) > **My profile**.

2. On the **Profile Settings** page, click the **Report Subscriptions** tab.

3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.

4. On the **Report Subscriptions** page, click **Edit** next to the report subscription that you want to edit.

5. In the details pane, under **Subscription Details**, 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.

   - **Additional subscribers**: Click **Assign**/**Change**, select the check box next to the identity who will also receive this report and click **Apply**.

     TIP: To remove a subscription, deselect the box next to the corresponding identity. To remove all subscriptions, click **Clear selection**. Click **Apply**.

6. (Optional) In the details pane under **Parameter**, specify any other report specific settings. These settings might vary depending on what report you use.

7. Click **Save**.

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 header, click 👤 (**Profile**) > **My profile**.

2. On the **Profile Settings** page, click the **Report Subscriptions** tab.

3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.

4. On the **Report Subscriptions** tab, perform the following:

   On the **Report Subscriptions** page, perform the following:

- To send the report, click ⋮ (**Actions**) > **Send report to me** next to the subscription of the report that you want to send.
- To send the report to all subscribers, click ⋮ (**Actions**) > **Send report to all subscribers** next to the subscription of the report you want to send.

Unsubscribing reports

You can unsubscribe reports.

To unsubscribe a report

1. In the header, click 👤 (**Profile**) > **My profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Report Subscriptions** tab, click ⋮ (**Actions**) > **Unsubscribe** next to the report subscription that you want to end.
5. In the **Unsubscribe Report** dialog, confirm the prompt with **OK**.

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 32
- Editing reports
- Generating reports on page 35
- Deleting reports on page 35
- 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 **Setup** > **Reports**.

2. On the **Reports** page, click **Create report**.

3. In the **Create Report** pane, enter the new report's main data.

Table 7: 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.

4. In the **Include data from the table** menu, select the base table whose content you want to include in the report.

5. Specify which information to include in the report. Then enter which columns of the base table to add to the report:

    a. Under **Columns to be included**, click **Add column**.

    b. In the menu, select the respective column.

    c. (Optional) To add another column to the report, repeat this step.

    TIP: To remove a column, click 🗑 (**Delete**).

    TIP: Drag and drop the columns to change their order.

6. (Optional) To place further restrictions on the data in the report, set conditions. Perform the following actions to do this:

    a. Under **Conditions**, click **Add condition**.

    b. In the **Property** menu, select the relevant property.

    c. In the **Operator** menu, select a logical operator.

    d. In the final field, specify a comparison value.

    e. (Optional) To add another condition to the report, repeat this step.

f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

| TIP: To remove a condition, click 🗑 (**Delete**).

For more information about customizing filter conditions, see Custom filter conditions.

7. Click **Create**.

Editing reports

You can edit your own reports.

To edit a report

1. In the menu bar click **Setup** > **Reports**.

2. On the **Reports** page, next to the report you want to edit, click **Edit**.

3. In the **Edit Report** pane, edit the report's main data.

Table 8: 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.

4. In the **Include data from the table** menu, select the base table whose content you want to include in the report.

5. Specify which information to include in the report. Then enter which columns of the base table to add to the report:

    a. Under **Columns to be included**, click **Add column**.

    b. In the menu, select the respective column.

c. (Optional) To add another column to the report, repeat this step.

| TIP: To remove a column, click 🗑 (**Delete**).

| TIP: Drag and drop the columns to change their order.

6. (Optional) To place further restrictions on the data in the report, set conditions. Perform the following actions to do this:

   a. Under **Conditions**, click **Add condition**.

   b. In the **Property** menu, select the relevant property.

   c. In the **Operator** menu, select a logical operator.

   d. In the final field, specify a comparison value.

   e. (Optional) To add another condition to the report, repeat this step.

   f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

   | TIP: To remove a condition, click 🗑 (**Delete**).

   For more information about customizing filter conditions, see Custom filter conditions.

7. Click **Save**.

Generating reports

You can generate reports and display the collected data.

To generate a report

1. In the header, click 👤 (**Profile**) > **My profile**.

2. On the **Profile Settings** page, click the **Report Subscriptions** tab.

3. On the **Report Subscriptions** tab, click **View a report**.

4. On the **View a Report** pane, click the report you want to generate.

5. In the **Format** menu, select the format to use to generate the report.

6. Click **Show report**.

   This downloads the report.

Deleting reports

You can delete reports.

To generate a report

1. In the menu bar click **Setup** > **Reports**.
2. On the **Reports** page, select the check box next to the report you want to delete.
3. Click **Delete**.
4. In the **Delete Reports** dialog, confirm the prompt with **Yes**.

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.

Work area

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

Detailed information about this topic

- Home on page 36
- Header on page 37
- Menu bar on page 37

Home

 Open the home page by clicking the company logo.

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 9: Functions in the header

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
Help	This menu includes online help, contact to customer service and information about the connection and the product. Use **Documentation** to open the context-sensitive help. The help contains the entire contents of the Web Portal User Guide. Here you can open the help. The help contains the entire contents of the Web Portal User Guide.

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. Click a menu in the menu bar.

   This expands the menu and shows more menu items.

2. Click a menu item.

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.

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 85).
- You are notified whether your request is granted or denied.

Detailed information about this topic

Setting up and configuring request functions

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

Application roles help you to define who can take over administrative tasks in the Web Portal.

Structure and workflow of requests

A shop is the top element in the hierarchical structure that is required for requesting products. A shop can contain several shelves. Products are assigned to these shelves and can then be requested.

Products can be grouped into service categories. Identities can select products from a service catalog in the Web Portal, add them to a cart, and submit a purchase request.

Requests follow a defined approval process that determines whether a product may be assigned or not. Authorized identities have the option to approve requests and cancellations. You determine which approval process to use by assigning approval policies to shops or shelves (see You can edit details of existing shops. on page 42 and Editing shelf details on page 45).

Detailed information about this topic

- Managing shops on page 39
- Managing service categories on page 49
- Managing service items
- Managing request templates

Managing shops

A shop is the top element in the hierarchical structure that is required for requesting products.

A shop can contain several shelves (see Managing shop shelves on page 43). Products are assigned to these shelves and can then be requested (see Managing requestable products in shops on page 48).

You can display, create, edit, or delete shops.

You can also decide who is able to request products from shops (see Managing access to requestable products in shops on page 46).

Detailed information about this topic

- Displaying shops on page 40
- Creating shops on page 40
- Editing shops on page 41
- Deleting shops on page 42
- Managing shop shelves on page 43
- Managing access to requestable products in shops on page 46
- Managing requestable products in shops on page 48

Displaying shops

You can display any of the shops and their details.

To display shops

1. In the menu bar click **Setup** > **Shops**.

   This opens the **Shops** page.

2. (Optional) To display details of a shop, in the list, click on the shop.

3. (Optional) You can perform the following actions:

   - You can see the shop's shelves (see You can display any of the shop's shelves and their details. on page 43).

   - You can display who can request products from the shop (see You can display the members of shops. These members can request products from the respective shop. on page 46).

Creating shops

To set up your own shop solution, you can create shops. You can then customize these shops as you wish (see Editing shops on page 41).

To create a shop

1. In the menu bar click **Setup** > **Shops**.

2. On the Shops page click **Create Shop**.

3. In the **Create Shop** pane, enter the main data for the new shop.

Table 10: Shop main data

Property	Description
Name	Enter a full, descriptive name for the shop.
Description	Enter a description for the shop.
Attestors	Click **Assign**/**Change** and select an application role. Members of this application role can approve attestation cases affecting products that can be requested through this shop.
	This setting is inherited by all the shelves that are assigned to this shop and do not have an attestor.
Approval policies	Click **Assign**/**Change** and select the check boxes in front of the approval policies used to determine the approvers if products are requested from this shop in the Web Portal. Click **Apply**.
	This setting is inherited by all the shelves that are assigned to this shop and do not have any approval policies.
Owner	Select the identity that is responsible for the shelf.
	The owner can be used as the approver in approval processes for requests from the shop.
2nd Manager	Select the identity that deputizes as the shop manager.
	The deputy can be used as the approver in approval processes for requests from the shop.

4. Click **Create**.

5. (Optional) Create shelves for the shop (see You can create shelves for shops and identities can request system entitlements from them. on page 43). In the shelves, you can specify which products can be requested from the shop (see Adding products to shelves on page 48).

6. (Optional) To specify who can request products from the shop, add members to the shop (see You can add members to shops. These identities can then request products from the respective shop. on page 46).

Editing shops

When you edit existing shops, you can perform the following actions:

- Edit shop details (see You can edit details of existing shops. on page 42)
- Manage shop shelves (see Managing shop shelves on page 43)
- Specify who can request products from shops (see Managing access to requestable products in shops on page 46)
- Specify which products can be requested from shops (see Managing requestable products in shops on page 48)

Editing shop details

You can edit details of existing shops.

To edit details of a shop

1. In the menu bar click **Setup** > **Shops**.

2. On the **Shops** page, in the list, click the shop whose details you want to edit.

3. In the **Edit Shop** pane, you can edit the main data of the shop.

Table 11: Shop main data

Property	Description
Name	Enter a full, descriptive name for the shop.
Description	Enter a description for the shop.
Attestors	Click **Assign**/**Change** and select an application role. Members of this application role can approve attestation cases affecting products that can be requested through this shop.
	This setting is inherited by all the shelves that are assigned to this shop and do not have an attestor.
Approval policies	Click **Assign**/**Change** and select the check boxes in front of the approval policies used to determine the approvers if products are requested from this shop in the Web Portal. Click **Apply**.
	This setting is inherited by all the shelves that are assigned to this shop and do not have any approval policies.
Owner	Select the identity that is responsible for the shelf.
	The owner can be used as the approver in approval processes for requests from the shop.
2nd Manager	Select the identity that deputizes as the shop manager.
	The deputy can be used as the approver in approval processes for requests from the shop.

4. Click **Save**.

Deleting shops

You can delete shops.

NOTE: Before you can delete a shop, you must delete all shelves from the shop (see You can delete shops. on page 45) and remove all members from the shop (see You can remove members from shops. These identities can then no longer request products from the shop. on page 47).

To delete a shop

1. In the menu bar click **Setup** > **Shops**.
2. On the **Shops** page, in the list, click the shop you want to delete.
3. In the **Edit Shop** pane, click **Delete Shop**.

Managing shop shelves

You can display, create, edit, or delete shop shelves.

Each shop contains a number of shelves from which identities can request products. There are various products available for request on shelves. Shelves are set up under each shop.

Detailed information about this topic

- You can display any of the shop's shelves and their details. on page 43
- You can create shelves for shops and identities can request system entitlements from them. on page 43
- When you edit the existing shelves of a shop, you can perform the following actions: on page 44
- Editing shelf details on page 45
- You can delete shops. on page 45

Displaying shop shelves

You can display any of the shop's shelves and their details.

You can display any of the shop's shelves and their details.

To display the shelves in a store

1. In the menu bar click **Setup** > **Shops**.
2. On the **Shops** page, in the list, click the shop whose shelves you want to display.
3. In the **Edit Shop** pane, click the **Shelves** tab.
4. (Optional) To display details of a shelf, click it in the list.
5. (Optional) You can display the products that can be requested over this shelf (see Displaying requestable products on page 48).

Creating shelves for shops

You can create shelves for shops and identities can request system entitlements from them.

To create a shelf for shop

1. In the menu bar click **Setup** > **Shops**.
2. On the **Shops** page, in the list, click the shop you want to create a shelf for.
3. In the **Edit Shop** pane, click the **Shelves** tab.
4. On the **Shelves** tab, click **Create shelf**.
5. In the **Create Shelf** pane, enter the main data for the new shelf.

Table 12: Shelves main data

Property	Description
Name	Enter a full, descriptive name for the shelf.
Description	Enter a description for the shelf.
Attestors	Click **Assign**/**Change** and select an application role. Members of this application role can approve attestation cases affecting products that can be requested over this shelf.
	This setting is inherited by all the products that are assigned to this shelf and do not have an attestor.
Approval policies	Click **Assign**/**Change** and select the approval policies that control how approvers are determined if products are requested from this shelf in the Web Portal.
	This setting is inherited by all the products that are assigned to this shop and do not have any approval policies.
Owner	Select the identity that is responsible for the shelf.
	The owner can be used as the approver in approval processes for off the shelf requests.
Deputy manager	Select the identity that deputizes for the shelf manager.
	The deputy can be used as the approver in approval processes for off the shelf requests.

6. Click **Create**.
7. (Optional) To specify which products can be requested from the shelf, add the corresponding products to the shelf (see Adding products to shelves on page 48).

Editing shop shelves

When you edit the existing shelves of a shop, you can perform the following actions:

- Edit shelf details (see You can edit details of existing shops. on page 42)
- Specify which products can be requested from shops (see Managing requestable products in shops on page 48)

Editing shelf details

You can edit details of existing shelves.

To edit details of a shelf

1. In the menu bar click **Setup** > **Shops**.
2. On the **Shops** page, in the list, click the shop whose shelf you want to edit.
3. In the **Edit Shop** pane, click the **Shelves** tab.
4. On the **Shelf** tab, in the list, click the shelf you want to edit.
5. In the **Edit shelf** pane, you can edit the main data of the shelf.

Table 13: Shelves main data

Property	Description
Name	Enter a full, descriptive name for the shelf.
Description	Enter a description for the shelf.
Attestors	Click **Assign**/**Change** and select an application role. Members of this application role can approve attestation cases affecting products that can be requested over this shelf.
	This setting is inherited by all the products that are assigned to this shelf and do not have an attestor.
Approval policies	Click **Assign**/**Change** and select the approval policies that control how approvers are determined if products are requested from this shelf in the Web Portal.
	This setting is inherited by all the products that are assigned to this shop and do not have any approval policies.
Owner	Select the identity that is responsible for the shelf.
	The owner can be used as the approver in approval processes for off the shelf requests.
Deputy manager	Select the identity that deputizes for the shelf manager.
	The deputy can be used as the approver in approval processes for off the shelf requests.

6. Click **Save**.

Related topics

- Managing requestable products in shops on page 48

Deleting shelves from shops

You can delete shops.

NOTE: Before you can delete a shelf, you must remove all the products from it (see Removing products from shelves on page 49).

To delete a shelf from a shop

1. In the menu bar click **Setup** > **Shops**.

2. On the **Shops** page, in the list, click the shop whose shelf you want to delete.

3. In the **Edit Shop** pane, click the **Shelves** tab.

4. On the **Shelves** tab, in the list, click the shelf you want to delete.

5. In the **Edit shelf** pane, click **Delete shelf**.

Managing access to requestable products in shops

You can define who can request products from shops. This you specify through memberships in the shop. Once an identity becomes a member of a shop, it can request products from the shop.

Detailed information about this topic

- You can display the members of shops. These members can request products from the respective shop. on page 46

- You can add members to shops. These identities can then request products from the respective shop. on page 46

- You can remove members from shops. These identities can then no longer request products from the shop. on page 47

Displaying shop members

You can display the members of shops. These members can request products from the respective shop.

To display members of a shop

1. In the menu bar click **Setup** > **Shops**.

2. On the **Shops** page, in the list, click the shop whose members you want to display.

3. In the **Edit Shop** pane, click the **Access** tab.

Adding members to shops

You can add members to shops. These identities can then request products from the respective shop.

To add a member to a shop

1. In the menu bar click **Setup** > **Shops**.

2. On the **Shops** page, in the list, click the Shop you want to add a member to.

3. In the **Edit Shop** pane, click the **Access** tab.

4. On the **Access** tab, click **Add members**.

5. In the **Add members** dialog, select the check box next to the identity that you want to add to the shop as a member.

6. Click **Apply**.

To add excluded members back into a shop

1. In the menu bar click **Setup** > **Shops**.

2. On the **Shops** page, in the list, click the Shop you want to add a member to.

3. In the **Edit Shop** pane, click the **Access** tab.

4. On the **Access** tab, click **Excluded members**.

5. Select the check box next to the identity that you want to add to the shop as a member.

6. Click **Remove exclusion**.

Removing members from shops

You can remove members from shops. These identities can then no longer request products from the shop.

> NOTE: You can exclude members who have been added to the shop through a dynamic role. You can add these excluded members back to the shop later (see You can add members to shops. These identities can then request products from the respective shop. on page 46). For more information about dynamic roles, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To remove a member from a shop

1. In the menu bar click **Setup** > **Shops**.

2. On the **Shops** page, in the list, click the Shop from which you want to remove a member.

3. In the **Edit Shop** pane, click the **Access** tab.

4. On the **Access** tab, in the list, select the check box next to the identity that you want to remove as a member.

5. Click **Remove**.

6. (Optional) If the member was assigned to the shop through a dynamic role, perform the following actions:

a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.

b. Click **Exclude members**.

Managing requestable products in shops

You can decide which products can be requested from shops. Once products have been allocated to shelves in a shop (see Making system entitlements requestable on page 232) and labeled as requestable , they can be requested in the Web Portal by members of the shop.

Detailed information about this topic

Displaying requestable products

You can display which products can be request from shops shelves.

To display a shelf's requestable products

1. In the menu bar click **Setup** > **Shops**.

2. On the **Shops** page, in the list, click the shop whose requestable products you want to display.

3. In the **Edit Shop** pane, click the **Shelves** tab.

4. On the **Shelves** tab, in the list, click the shelf with the requestable products you want to display.

5. In the **Edit shelf** pane, click the **Products** tab.

Adding products to shelves

You can add products to shelves. Once products have been allocated to the shelves of a shop, they can be requested in the Web Portal by members of the shop.

To add a product to a shelf

1. In the menu bar click **Setup** > **Shops**.

2. On the **Shops** page, in the list, click the shop that you want request the product from later.

3. In the **Edit Shop** pane, click the **Shelves** tab.

4. On the **Shelves** tab, in the list, click the shelf you want to add the product to.

5. In the **Edit shelf** pane, click the **Products** tab.

6. On the **Products** tab, click **Add products**.

7. In the **Add Products** dialog, select the type of product you want to add from the menu.

8. Select the check box next to the product that you want to add to the shelf.

9. Click **Apply**.

Removing products from shelves

You can remove products from shelves, after which they can no longer be requested from the shelves.

To remove a product from a shelf

1. In the menu bar click **Setup** > **Shops**.

2. On the **Shops** page, in the list, click the shop from whose shelf you want to remove the product.

3. In the **Edit Shop** pane, click the **Shelves** tab.

4. On the **Shelves** tab, in the list, click the shelf to remove the product from.

5. In the **Edit shelf** pane, click the **Products** tab.

6. On the **Products** tab, select the check box next to the product that you want to remove from the shelf.

7. Click **Remove**.

Managing service categories

Use the Web Portal to display and edit service categories.

Service categories are used to group products. For example, you can use service categories to group together products by topic.

You can assign the product's service items to these service categories (see Editing system entitlement service items on page 239).

Detailed information about this topic

- Displaying service categories on page 50
- Creating service categories on page 50
- Editing service categories on page 52
- Deleting service categories on page 54

Displaying service categories

You can display any of the service categories and their details.

To display service categories

1. In the menu bar, click **Setup** > **Service categories**.

   This opens the **Service Categories** page and displays all the service categories.

2. (Optional) To display the details of a service category, next to the service category, click **Edit**.

Creating service categories

You can create service categories.

To create a service category

1. On the menu bar, click **Setup** > **Service categories**.

2. On the **Service Categories** page, click **Create service category**.

3. In the **Create Service Category** pane, enter the service category's main data.

Table 14: Service category main data

Property	Description
Service category	Enter a full, descriptive name for the service category.
Description	Enter a description for the service category.
Parent service category	To structure service categories hierarchically, click **Assign**/**Change** and then select the parent service category.
Attestors	Click **Assign**/**Change** and then select an application role. Members of this application role can approve attestation cases that affect the service category.
Product owners	Click **Assign**/**Change** and then select an application role. Members of this application role can edit the service category's main data. They can also be used as approvers in approval processes when requests for service items assigned to this service category.
Approval policies	Select the approval policy used to determine the approver when the service item is requested in the Web Portal. NOTE: The approval policy specified for a service category is inherited by all associated service items and all child service categories where this is not specified.
Sort order	Enter the way you want the service category's service items to be sorted.
Picture	Add a picture of the service category. Users see this picture when they make a request. If you do not insert a picture here, the picture of the assigned service category is used. Perform the following actions to do this: 1. Click **Add**/**Change**. 2. Select an image from your medium.
Application	To assign an application to a service category, select the application.
Service items	Specify the products can be requested through the service category. Perform the following actions as well: 1. Click **Assign**/**Change**. 2. Select the check box next to the service item you want to assign to the service category.

Property	Description
	TIP: To remove a service item, deselect the relevant check box in front of the service item. To remove all service items, click **Clear selection**.

3. Click **Apply**.

4. Click **Save**.

Editing service categories

You can edit service items.

To edit a service category

1. On the menu bar, click **Setup** > **Service categories**.

2. On the **Service Categories** page, next to the service category you want to edit, click **Edit**.

3. In the **Edit Service Category** pane, enter the service category's main data.

Table 15: Service category main data

Property	Description
Service category	Enter a full, descriptive name for the service category.
Description	Enter a description for the service category.
Parent service category	To structure service categories hierarchically, click **Assign**/**Change** and then select the parent service category.
Attestors	Click **Assign**/**Change** and then select an application role. Members of this application role can approve attestation cases that affect the service category.
Product owners	Click **Assign**/**Change** and then select an application role. Members of this application role can edit the service category's main data. They can also be used as approvers in approval processes when requests for service items assigned to this service category.
Approval policies	Select the approval policy used to determine the approver when the service item is requested in the Web Portal. NOTE: The approval policy specified for a service category is inherited by all associated service items and all child service categories where this is not specified.
Sort order	Enter the way you want the service category's service items to be sorted.
Picture	Add a picture of the service category. Users see this picture when they make a request. If you do not insert a picture here, the picture of the assigned service category is used. Perform the following actions to do this: 1. Click **Add**/**Change**. 2. Select an image from your medium.
Application	To assign an application to a service category, select the application.
Service items	Specify the products can be requested through the service category. Perform the following actions as well: 1. Click **Assign**/**Change**. 2. Select the check box next to the service item you want to assign to the service category.

ONE IDENTITY
by Quest

Property	Description
	TIP: To remove a service item, deselect the relevant check box in front of the service item. To remove all service items, click **Clear selection**.

3. Click **Apply**.

4. Click **Save**.

Deleting service categories

You can delete existing service categories.

Before you can delete a service category, the following requirements must be met:

- The service category is not predefined. Whether a service category is predefined, you can see from the description (see Displaying service categories on page 50).

- Service items are no longer assigned to the service category. To remove service items, edit the service category and remove the assigned service items (see Editing service categories on page 52).

- There are no longer child service categories under the service category. To assign child service categories under another service category or to remove them again, edit the corresponding child service category and remove or change the parent service category (see Editing service categories on page 52).

To delete a service category

1. On the menu bar, click **Setup** > **Service categories**.

2. On the **Service Categories** page, next to the service category you want to delete, click **Edit**.

3. In the **Edit Service Category** pane, click **Delete service category**.

4. In the **Delete Service Category** dialog, confirm the prompt with **Yes**.

Managing service items

Use the Web Portal to display and edit service items.

In order to request company resources in the Web Portal, a service item must be assigned to them. Service items contain additional information about company resources (for example, article number, request properties, product manager or approver for requests).

Detailed information about this topic

-
-
-
-

Displaying service items

You can display all service items.

To display all service items

1. In the menu bar, click **Setup** > **Service items**.

   This opens the **Service Items** page and displays all the service items.

2. (Optional) To display details of a service item, next to the service item, click **Edit**.

Editing service items

You can display all service items.

To display all service items

1. In the menu bar, click **Setup** > **Service items**.
2. On the **Service Items** page, next to the service item, click **Edit**.
3. In the **Service Item** pane, edit the service item's main data.

Table 16: Main data of system entitlement service items

Property	Description
Service item	Enter a name for the service item.
Description	Enter a description of the service item.
Service category	You can group different service items into service categories. To do this, click **Assign**/**Change** and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 49.
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the

Property	Description
	Web Portal.
Approval by multi-factor authentication	Select this check box to specify that approvals of requests for this service item require multi-factor authentication.
Max. days valid	Specify how long an identity can keep the product until it is automatically unsubscribed again.
	An identity keeps their requested products on the shelf until they unsubscribe from them themselves. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. Products that are intended to have a limited shelf life need to be marked with a validity period.
Website	Specify the URL of a web page that contains more information about the product. Use the following format: **https://www.example.com** or **http://www.example.com**.
	This field allows you to link product descriptions in the internet or intranet to the service item.
Sort order	Specify how the service category is sorted.
Request property	Select the request property using the additional request parameters that are defined for a request. If you do not select any request properties, the request properties of the associated service category are used.
	Requests can be given additional information though product-specific request properties such as the specific details of a product, its size, or color. A request property gathers all additional features together that can be given when requesting a product.
Functional area	Click **Assign**/**Change** and then select the functional area to which you want to assign the service item.
	You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by functional area. To do this, service items must be assigned to functional areas. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Attestors	Click **Assign**/**Change** and then select an application role. Members of this application role can approve

Property	Description
	attestation cases that affect the service item.
Terms of use	Select the terms of use that the product's requester must accept.
Picture	Enter a picture for the service item. Users see this picture when they make a request. Perform the following actions as well: 1. Click **Add**/**Change**. 2. Select an image from your medium.
Request parameters must be defined per recipient	Select the check box to enter additional request properties separately for each recipient of this product, if the product is requested for different recipients in one request procedure.
Retain service item assignment on relocation	Select the check box if requests for this service item are retained when a customer or the product is moved. If an identity requests a product from a Shop and changes the Shop at a later date, a decision must be made about how to proceed with the existing request. The same applies if a product is moved to another shelf.
Tags	Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.
Not requestable/Requestable	Set the switch to **Requestable** if you want to request system entitlements through the Web Portal. Set the switch to **Not requestable** if you do not want to request system entitlements through the Web Portal. For more information, see Making system entitlements requestable on page 232.
Product owner	Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item. Specify which identities are responsible for the service item. • To specify members of a specific application role as product owners, perform the following under **Product owners**:

ONE IDENTITY
by Quest

Property	Description

	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.

4. Click **Save**.

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 72
- Displaying request templates
- Creating request templates on page 59
- Sharing request templates on page 60
- Editing request templates on page 59
- Deleting request templates on page 61

Displaying request templates

To obtain an overview of all the request templates, you can display them and their associated content.

To display request templates

1. In the menu bar, click **Setup** > **Request templates**.

   This opens the **Request Templates** page.

2. (Optional) To display the details of a request template, next to the request template, click **Edit**.

3. (Optional) To display the products in the request template, in the **Edit Request Template** pane, click the **Products** tag.

Related topics

- Requesting using request templates on page 72

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.

To create a request template from the shopping cart

1. In the menu bar, click **Requests** > **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 62).

2. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you want to add to the request template.

3. On the **Shopping Cart** page, click ⋮ (**Actions**) > **Create request template**.

4. In the **Create Request Template** pane, in the **Request template** field, enter a meaningful name for the request template.

5. (Optional) In the **Description** field, enter a description for the request template.

6. Click **Create**.

Related topics

- Requesting using request templates on page 72

Editing request templates

You can edit the details of your request templates. You can also remove products from request templates that you created yourself (see Removing products from request templates on page 60).

To edit a request template

1. In the menu bar, click **Setup** > **Request templates**.

2. On the **Request Templates** page, next to the request template you want to edit, click **Edit**.

   | NOTE: You can only edit request templates that you created yourself.

3. In the **Edit Request Template** pane, enter any additional information you want provide.

   | TIP: You can also share request templates with other users here (see Sharing request templates).

Detailed information about this topic

- Removing products from request templates on page 60

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 **Setup** > **Request templates**.

2. On the **Request Templates** page, next to the product you want to remove, click **Edit**.

   | NOTE: You can only edit request templates that you created yourself.

3. In the **Edit Request Template** pane, click the **Products** tab.

4. On the **Products** tab, select the check box next to the product that you want to remove.

5. Click **Remove**.

Related topics

- Requesting using request templates on page 72

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 **Setup** > **Request templatesRequests** > **My request templates**.

2. On the **Request Templates** page, select the check box next to the request template you want to share with other users.

3. Click **Share**.

Related topics

- Requesting using request templates on page 72

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 **Setup** > **Request templates**.

2. On the **Request Templates** page, next to the request template you want to delete, click **Edit**.

3. In the **Edit Request Template** pane, click **Delete**.

4. In the **Delete Request Template** dialog, confirm the prompt with **Yes**.

Related topics

- Requesting using request templates on page 72

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 62).

2. Verify the shopping cart and amend the product requests as required (see Managing products in the shopping cart on page 63).

3. Submit the request (see Submitting requests on page 69).

Detailed information about this topic

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 **Requests** > **New request**.

   This opens the **New Request** page and displays all the available products.

2. (Optional) To filter which products are displayed, perform one of the following actions:

   - In the search field, enter the name of a product you want to look for.
   - Click **Show products from service category** and then select the service category containing the products you want to display.

   The relevant products are displayed.

   > TIP: To change the service category you have selected, click ⊗ (**Delete filter**) next to the selected service category and then select another service category using **Show products from service category**.
   >
   > 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.

3. Perform one of the following tasks:

   - In the tile view (▦)

     - Add a product to the shopping cart: On the tile with the product you want to request, click **Add to cart**.
     - Add multiple products to the shopping cart: Click the tile with the products you want to request and click **Add to cart** below the list.

> **TIP:** To select all the displayed products, next to **Selected products**, click **Select all on page**.
>
> To remove the product selection, next to **Selected products**, click **Deselect all**.

- In the list view (≣)

    - 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 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.

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 63). Then send the request (see Submitting requests on page 69).

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 63
- Submitting requests on page 69

Managing products in the shopping cart

After you have added products to your shopping cart (see Adding products to the shopping cart on page 62), 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 **Requests** > **Shopping cart**.

2. 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 65)

- Define the validity of the products (see Setting the validity period of products in your shopping cart on page 65)
- Change the priority of the requests (see Specifying the priority of products in your shopping cart on page 66)
- Enter reasons for the requests (see Giving reasons for requests on page 67)
- Check the shopping cart for invalid products and remove them (see Checking the shopping cart on page 67)
- Request products for multiple identities (see Requesting products in the shopping cart for multiple identities on page 68)
- Place products on the Saved for Later list (see Saving products for later on page 79)
- Show the Saved for Later list (see Displaying Saved for Later list on page 80)

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

   Now you can send your request (see Submitting requests on page 69).

Related topics

- Adding products to the shopping cart on page 62
- Submitting requests on page 69
- Saved for Later list on page 79

Displaying the shopping cart

After you have added products to your shopping cart (see Adding products to the shopping cart on page 62), 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 **Requests** > **Shopping cart**.

   This opens the **Shopping Cart** page.

2. 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 62
- Submitting requests on page 69

Removing products from the shopping cart

After adding added products to your shopping cart (see Adding products to the shopping cart on page 62), you can remove them again.

To remove products from the shopping cart

1. In the menu bar, click **Requests** > **Shopping cart**.

2. On the **Shopping Cart** page, click **Remove from cart** next to the product that you do not want to request anymore.

3. In the **Remove Product From Cart** 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 multiple products from the shopping cart

1. In the menu bar, click **Requests** > **Shopping cart**.

2. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you do not want to request anymore.

3. Click ⋮ (**Actions**) > **Remove selected**.

4. In the **Remove Selected Products From Cart** 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 68.

Related topics

- Adding products to the shopping cart on page 62
- Submitting requests on page 69

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 62), 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 96.

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

1. In the menu bar, click **Requests** > **Shopping cart**.

2. On the **Shopping Cart** page, in the list, click **Edit** next to the product whose validity period you want define.

3. In the details pane, in the **Valid from** field, specify from when the product is valid.

4. In the **Valid until** field, specify until when the product is valid.

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 62
- Submitting requests on page 69

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 62), 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 **Requests** > **Shopping cart**.

2. On the **Shopping Cart** page, click **Edit** next to the product whose priority you want define.

3. In the details pane, in the **Priority** menu, select the priority.

4. 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 62
- Submitting requests on page 69

Giving reasons for requests

After you have added products to your shopping cart (see Adding products to the shopping cart on page 62), 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 **Requests** > **Shopping cart**.

2. On the **Shopping Cart** page, click **Edit** next to the product with the request you want to justify.

3. In the details pane, in the **Reason** field, enter your reason for requesting this product.

4. 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 62
- Submitting requests on page 69

Checking the shopping cart

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.

To check your shopping cart for invalid products

1. In the menu bar, click **Requests** > **Shopping cart**.

2. On the **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, an appropriate message appears in the **Check result** column next to the invalid product.

3. In the list, click **Error** next to the invalid product.

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

Related topics

- Adding products to the shopping cart on page 62
- Submitting requests on page 69

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 62), 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 **Requests** > **Shopping cart**.

2. On the **Shopping Cart** page, click **Edit** next to the product that you want to request for other identities.

3. In the details pane, click **Actions** > **Request for multiple identities**.

4. In the **Request for Multiple Identities** pane, select the check boxes next to the identities you want to request the product for.

5. Click **Apply**.

6. Close 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

- Requesting for other identities or subidentities on page 69
- Adding products to the shopping cart on page 62
- Submitting requests on page 69

Deleting shopping carts

You can clear your shopping cart at any time.

To delete your shopping cart

1. In the menu bar, click **Requests** > **Shopping cart**.

2. On the **Shopping Cart** page, click ⋮ (**Actions**) > **Delete shopping cart**.

3. In the **Delete Shopping Cart** dialog, confirm the prompt with **Yes**.

Related topics

- Removing products from the shopping cart on page 65
- Adding products to the shopping cart on page 62

Submitting requests

After you have added products to your shopping cart (see Adding products to the shopping cart on page 62), and edited and, if necessary, checked the request (see Managing products in the shopping cart on page 63), you can submit your shopping cart.

To submit your requests

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

   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 on page 67 and Removing products from the shopping cart on page 65).

Related topics

- Adding products to the shopping cart on page 62
- Managing products in the shopping cart on page 63
- Checking the shopping cart on page 67
- Removing products from the shopping cart on page 65

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 68.

To request products for another identity

1. In the menu bar, click **Requests** > **New request**.

2. On the **New Request** page, enable the **For others** option.

3. In the **Recipients** field, click **Assign**.

4. In the **Change recipient** pane, in the list, select the check boxes next to the identity you want to request products for.

   TIP: To remove an identity from the recipient list, deselect the check box next to the identity.

   TIP: To view only your subidentities, click ▼ (**Filter**) and then select the **My sub identities** check box.

5. Click **Apply**.

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 62).

7. (Optional) Edit the shopping cart (see Managing products in the shopping cart on page 63).

8. Submit the request (see Submitting requests on page 69).

Related topics

- Requesting products in the shopping cart for multiple identities on page 68

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 68

- Requesting for other identities or subidentities on page 69

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 **Requests** > **New request**.

2. On the /**New Request** page, click ⋮ (**Actions**) > **Select a reference user**.

3. In the **Select Reference User** dialog, click **Assign** next to the identity whose products you also want to request.

   This opens the **New Request - By Reference User** page that, on the **Products** and **Organizational Structures** tabs, lists the requests, memberships, and entitlements of the selected identity.

4. Add the products that you want to save for later, to the shopping cart (see Adding products to the shopping cart on page 62).

5. 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 63.

Related topics

- Requesting products through peer groups on page 71
- Managing products in the shopping cart on page 63

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 **Requests** > **New request**.

2. (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 **New Request** page, enable the **For others** option.

   b. In the **Recipients** field, click **Assign**.

c. In the **Change recipient** pane, in the list, select the check boxes next to the identity you want to request products for.

> NOTE: The list may contain a maximum of one identity. To remove an identity from the list, clear the check box next to the respective identity.

d. Click **Apply**.

3. On the **New Request** page, click ⋮ (**Actions**) > **Show products other identities requested**.

This opens the **New Request - By Peer Group** page that, on the **Products** and **Organizational Structures** tabs, lists requests, memberships, and the peer group entitlements of the selected identity.

4. Add the products that you want to save for later, to the shopping cart (see Adding products to the shopping cart on page 62).

5. 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 63.

Related topics

- Requesting products through reference users on page 71
- Managing products in the shopping cart on page 63

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 71.

To request products using a request template

1. In the menu bar, click **Requests** > **New request**.

2. On the **New Request** page, click the **Request Templates** tab.

3. (Optional) On the **Request Templates** tab, select which request templates you want to display:

   - **All request templates**: Displays all available request templates (private and public).

- **Public request templates**: Displays all request templates that users have shared with other users.
- **Private request templates**: Displays all request templates that you have created and not shared with other users.

4. To add products from request templates in the shopping cart, perform the following actions:

- In the tile view (⊞)

  - Select a request template: In the tile of the request template whose products you want to request, click **Add to cart**.

  - Select multiple request templates: Click the tiles of the request templates whose products you want to request, then below the list, click **Add to cart**.

- In the list view (☰)

  - Select a request template: Next to the request template whose products you want to request, click **Add request template products to cart**.

  - Select multiple request templates: Next to the request templates whose products you want to request, select the check box, then below the list, click **Add to cart**.

  TIP: To select all the displayed request templates, next to **Selected products**, click **Select all on page**.

  To remove the request template selection, next to **Selected products**, click **Deselect all**.

  TIP: If you want to see which products are contained in a request template, click **Details**.

5. On the **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 63.

Related topics

- Managing request templates
- Managing my request templates
- Managing products in the shopping cart on page 63
- Requesting products through reference users on page 71

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 **Requests** > **New request**.

2. On the **New Request** page, click **Show products from service category**.

3. In the **Service category** pane, click **Privileged access requests**.

4. On the **New 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 **Request Details** pane, expand the selected product.

7. In the **PAM user account** menu, 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 or SSH key request:

     1. In the **System to access** field, click **Assign**.

     2. In the **System to access** pane, select whether you want to request access for a **PAM asset** or a **PAM directory**.

     3. Next to the corresponding PAM directory or PAM asset, click **Assign**.

   - Remote desktop session request, SSH session request, or Telnet session request: In the **System to access**, select the corresponding PAM asset.

9. Perform the following actions:

   a. In the **Account to access** field, click **Assign**.

   b. In the **Account for access** pane, select whether you want to request access for a **PAM asset account** or a **PAM directory account**.

   c. Next to the corresponding PAM asset account or PAM directory account, click **Assign**.

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.

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 **Apply**.

14. (Optional) Repeat the steps for all other users and access types.

15. Click **Submit**.

16. On the **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 63.

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 95) 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 63

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 75
- Requesting changes to Active Directory groups on page 76
- Requesting deletion of Active Directory groups on page 77

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 **Requests** > **New request**.

2. On the **New Request** page, click **Show products from service category**.

3. In the **Service category** pane, click the **Active Directory groups** service category.

4. Perform one of the following actions:

- To request a new Active Directory security group, click the **New Active Directory security group** tile.

- To request a new Active Directory distribution group, click the **New Active Directory distribution group** tile.

5. Click **Add to cart**.

6. In the **Request Details** pane, perform one of the following actions:

   - As a requester without responsibility for the target system, enter a 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.

7. Click **Apply**.

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 63.

9. On the **Shopping Cart** page, click **Submit**.

Related topics

- Approving pending requests from newly created Active Directory groups on page 87

Requesting changes to Active Directory groups

To change the type or scope of Active Directory groups, you must request the **Change an Active Directory group** product.

To change an Active Directory group

1. In the menu bar, click **Requests** > **New request**.

2. On the **Request** page, click **Show products from service category**.

3. In the **Service category** pane, click the **Active Directory groups** service category.

4. Click the **Modify Active Directory group** tile.

5. Click **Add to cart**.

6. In the **Request Details** pane, in the **Active Directory group** menu, select the Active Directory group that you want to change.

7. (Optional) In the **Group scope** menu, 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.

8. (Optional) In the **Type** menu, select the type of Active Directory group (security or distribution group).

9. Click **Apply**.

10. 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 63.

11. On the **Shopping Cart** page, click **Submit**.

Requesting deletion of Active Directory groups

To delete Active Directory groups you must request the **Delete Active Directory group** product.

To delete an Active Directory group

1. In the menu bar, click **Requests** > **New request**.

2. On the **New Request** page, click **Show products from service category**.

3. In the **Service category** pane, click the **Active Directory groups** service category.

4. Click the **Delete Active Directory Group** tile.

5. Click **Add to cart**.

6. In the **Request Details** pane, in the **Active Directory group to delete** menu, select the Active Directory group that you want to delete.

7. Click **Apply**.

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 63.

9. On the **Shopping Cart** page, click **Submit**.

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 **Requests** > **New request**.

2. On the **New Request** page, click **Show products from service category**.

3. In the **Service category** pane, click the **SharePoint groups** service category.

4. Click the **New SharePoint group** tile.

5. Click **Add to cart**.

6. In the **Request Details** pane, perform one of the following actions:

   - As a requester without responsibility for the target system, enter a name for the new group in the **Suggested name** field.

   - As the target system manager, provide additional details 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.

7. Click **Apply**.

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 63.

9. On the **Shopping Cart** page, click **Submit**.

Related topics

- Approving pending requests from newly created SharePoint groups on page 88

Saved for Later list

In your Saved for Later list you can save products that you want to request at a later date.

Detailed information about this topic

- Saving products for later on page 79
- Displaying Saved for Later list on page 80
- Requesting products on the Saved for Later list on page 80
- Removing products from the Saved for Later list on page 81
- Deleting the Saved for Later list on page 82

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 80).

To add products to your Saved for Later list.

1. Add the products that you want to save for later, to the shopping cart (see Adding products to the shopping cart on page 62).

2. In the menu bar, click **Requests** > **Shopping cart**.

3. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you want to save for later.

4. Click ⋮ (**Actions**) > **Move to Saved for Later list**.

   The products are moved with all their settings to your shopping cart.

Related topics

- Managing products in the shopping cart on page 63

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 **Requests** > **Shopping cart**.

2. On the **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 **View Saved for Later list**.

Related topics

- Managing products in the shopping cart on page 63

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 **Requests** > **Shopping cart**.

2. On the **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 **View Saved for Later list**.

3. 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.

4. Click ⋮ (**Actions**) > **Move to shopping cart**.

   This moves the products and all their settings to your shopping cart.

5. On the **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 63.

Related topics

- Managing products in the shopping cart on page 63
- Submitting requests on page 69

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 82.

To remove a product from your Saved for Later list

1. In the menu bar, click **Requests** > **Shopping cart**.

2. On the **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 **View Saved for Later list**.

3. On the **Saved for Later** page, click **Remove from list** next to the product you want to remove from the Save for Later list.

4. In the **Remove Product From Saved For Later List** dialog, confirm the prompt with **Yes**.

To remove multiple products from your Saved for Later list

1. In the menu bar, click **Requests** > **Shopping cart**.

2. On the **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 **View Saved for Later list**.

3. 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.

4. Click ⋮ (**Actions**) > **Remove selected**.

5. In the **Remove Selected Products From Saved For Later List** dialog, confirm the prompt with **Yes**.

Related topics

- Managing products in the shopping cart on page 63

ONE IDENTITY by Quest

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 81.

To delete your Saved for Later list

1. In the menu bar, click **Requests** > **Shopping cart**.

2. On the **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 **View Saved for Later list**.

3. On the **Saved for Later** page, click **Delete Saved for Later list**.

4. In the **Delete Saved for Later List** dialog, confirm the prompt with **Yes**.

Related topics

- Managing products in the shopping cart on page 63

Managing my 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 72
- Displaying my request templates
- Creating my request templates on page 83
- Editing my request templates on page 83
- Sharing my request templates
- Deleting my request templates on page 85

Displaying my request templates

To obtain an overview of your request templates, you can display them and their associated content.

To display request templates

1. In the menu bar, click **Requests** > **My request templates**.

   This opens the **Request Templates** page.

2. (Optional) To display the details of a request template, next to the request template, click **Edit**.

3. (Optional) To display the products in the request template, in the **Edit Request Template** pane, click the **Products** tag.

Related topics

- Requesting using request templates on page 72

Creating my 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.

To create a request template from the shopping cart

1. In the menu bar, click **Requests** > **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 62).

2. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you want to add to the request template.

3. On the **Shopping Cart** page, click ⋮ (**Actions**) > **Create request template**.

4. In the **Create Request Template** pane, in the **Request template** field, enter a meaningful name for the request template.

5. (Optional) In the **Description** field, enter a description for the request template.

6. Click **Create**.

Related topics

- Requesting using request templates on page 72

Editing my request templates

You can edit the details of your request templates. You can also remove products from request templates that you created yourself (see Removing products from request templates on page 60).

To edit a request template

1. In the menu bar, click **Requests** > **My request templates**.

2. On the **Request Templates** page, next to the request template you want to edit, click **Edit**.

   NOTE: You can only edit request templates that you created yourself.

3. In the **Edit Request Template** pane, enter any additional information you want provide.

   TIP: You can also share request templates with other users here (see Sharing my request templates).

Detailed information about this topic

- Removing products from my request templates

Removing products from my request templates

You can remove products from your request templates.

To remove a product from a request template

1. In the menu bar, click **Requests** > **My request templates**.

2. On the **Request Templates** page, next to the product you want to remove, click **Edit**.

   NOTE: You can only edit request templates that you created yourself.

3. In the **Edit Request Template** pane, click the **Products** tab.

4. On the **Products** tab, select the check box next to the product that you want to remove.

5. Click **Remove**.

Related topics

- Requesting using request templates on page 72

Sharing my 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 **Requests** > **My request templates**.

2. On the **Request Templates** page, select the check box next to the request template you want to share with other users.

3. Click **Share**.

Related topics

- Requesting using request templates on page 72

Deleting my 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 **Requests** > **My request templates**.

2. On the **Request Templates** page, select the check box next to the request template you want to delete.

3. Click **Delete**.

4. In the **Delete Request Templates** dialog, confirm the prompt with **Yes**.

Related topics

- Requesting using request templates on page 72

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.

Detailed information about this topic

- Displaying pending requests on page 86
- Approving and denying requests on page 86

- Appointing other approvers for pending requests on page 90
- Rejecting request approval on page 94

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 86).

You can also display request that you have placed that still need to be granted or denied approval by others.

To display pending requests

1. In the menu bar, click **Requests** > **Pending requests**.

   This opens the **Pending Requests** page.

2. (Optional) To display details of a pending request, click **Details** next to the request whose details you want to see.

To display your pending requests so that others can grant or deny approval.

1. Open the home page.

2. On the home page, click **EXPLORE** in the **My Pending Requests** tile.

   This opens the **Request History** page and display requests that you have made but still need to be granted or denied approval by someone else (see Displaying request history on page 95).

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 **Requests** > **Pending requests**.

2. (Optional) To approve a request as a member of the chief approval team and only display the relevant requests, on the **Pending Requests** page, select the **Show requests to be approved by chief approval team** check box.

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 approve or deny multiple requests, in the table, select the check boxes next to the products and, below the table, click **Approve** or **Deny**.

4. (Optional) On the **Approve Request**/**Deny Request** page, perform the following actions:

   a. In the **Reason for your decision** field, select a standard reason for your approval decision.

   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

5. (Optional) To specify a validity period for the requested product, perform the following actions:

   a. In the **Valid from** field, specify from when the products are is valid.

   b. In the **Valid until** field, specify until when the product is valid.

6. Click **Save**.

Related topics

- Approving new managers' pending requests on page 89

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 **Requests** > **Pending requests**.

2. On the **Pending Requests** page, click **Approve** next to the request for a new Active Directory group.

3. In the **Approve Request** section, 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,

ONE IDENTITY
by Quest

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.

4. (Optional) To specify a validity period for the Active Directory group, perform the following actions:

   a. In the **Valid from** field, specify as from when the Active Directory groups are valid.

   b. In the **Valid until** field, specify until when the Active Directory groups are valid.

5. (Optional) Perform one of the following actions:

   a. In the **Reason for your decision** field, select a standard reason for your approval decision.

   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

   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

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 **Requests** > **Pending requests**.

2. On the **Pending Requests** page, click **Approve** next to the request for a new SharePoint group.

3. In the **Approve Request** section, 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.

4. (Optional) To specify a validity period for the SharePoint group, perform the following actions:

   a. In the **Valid from** field, specify as from when the SharePoint groups are valid.

   b. In the **Valid until** field, specify until when the SharePoint groups are valid.

5. (Optional) Perform the following actions:

   a. In the **Reason for your decision** field, select a standard reason for your approval decision.

   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

   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

- Requesting new SharePoint groups on page 78

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 167). 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 **Requests** > **Pending requests**.

2. On the **Pending Requests** page, next to the **New manager assignment** request, click **Approve**.

3. In the **Approve Request** page, expand the **New manager assignment** pane.

4. (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, disable the check boxes next to the respective entitlements and products.

5. (Optional) To specify from when the new manager is responsible for the identity, enter the date in the **Valid from** field. If you leave the field blank, the change of manager will be carried out immediately after approval.

6. (Optional) In the **Approve Request** pane, perform the following actions:

   a. In the **Reason for your decision** field, select a standard reason for your approval decision.

   b. In the **Additional comments about your decision** field, enter extra information about your approval decision.

7. Click **Save**.

Related topics

- Assigning other managers to my identities on page 167

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 91).

- Appoint additional approver
  You can give an another identity the task of approving (see Appointing additional approvers to pending requests on page 91). 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 94).
  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 93). 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 94).

You can withdraw a delegation and delegate another identity. For example, if the other approver is not available.

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 **Requests** > **Pending requests**.
2. On the **Pending Requests** page, click **Details** next to the request whose approval you want to reroute.
3. In the **View Request Details** pane, click **Reroute approval**.
4. In the **Reroute approval** pane, in the **Select approval level** menu, select the approval level you want to reroute to.
5. (Optional) In the **Reason for your decision** field, enter a reason for rerouting.
6. Click **Save**.

To reroute multiple approvals

1. In the menu bar, click **Requests** > **Pending requests**.
2. On the **Pending Requests** page, in the list, select the check boxes next to the requests whose approvals you want to reroute.
3. Click ⋮ (**Actions**) > **Reroute approval**.
4. In the **Reroute Approval** pane, in the **Select approval level** menu, select the respective approval level to reroute to.
5. (Optional) In the **Reason for your decision** field, enter a reason for rerouting.
6. Click **Save**.

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 **Requests** > **Pending requests**.
2. On the **Pending Requests** page, in the list, click **Details** next to the request to which you want to add an additional approver.
3. In the **View Request Details** pane, click **Add approver**.

4. In the **Add Additional Approver** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.

5. In the **Reason for your decision** field, select a standard reason for adding an additional approver.

6. Click **Save**.

To add an additional approver to multiple requests

1. In the menu bar, click **Requests** > **Pending requests**.

2. On the **Pending Requests** page, in the list, select the check boxes next to the requests to which you want to add an additional approver.

3. Click ⋮ (**Actions**) > **Add approver**.

4. In the **Add Additional Approver** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.

5. In the **Reason for your decision** field, select a standard reason for adding an additional approver.

6. Click **Save**.

Related topics

- Removing additional approvers of pending requests on page 92

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.

To withdraw a request's additional approver

1. In the menu bar, click **Requests** > **Pending requests**.

2. On the **Pending Requests** page, click **Details** next to the request to which you added an additional approver.

3. In the **View Request Details** pane, click **Withdraw additional approver**.

4. In the **Withdraw Additional Approver** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.

5. Click **Save**.

To withdraw additional approver from multiple requests

1. In the menu bar, click **Requests** > **Pending requests**.

2. On the **Pending Requests** page, in the list, select the check boxes next to the requests to which you added an additional approver.

3. Click ⋮ (**Actions**) > **Withdraw additional approver**.

4. In the **Withdraw Additional Approver** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.

5. Click **Save**.

Related topics

- Appointing additional approvers to pending requests on page 91

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 94).

To delegate an approval

1. In the menu bar, click **Requests** > **Pending requests**.

2. On the **Pending Requests** page, click **Details** next to the request whose approval decision you want to delegate to another identity.

3. In the **View Request Details** pane, click **Delegate approval**.

4. In the **Delegate approval**, in the **Delegate to** menu, select the identity to which you want to delegate the approval.

5. In the **Reason for your decision** field, enter a reason for the delegation.

6. Click **Save**.

To delegate approval of multiple requests

1. In the menu bar, click **Requests** > **Pending requests**.

2. On the **Pending Requests** page, in the list, select the check boxes next to the requests whose approval you want to delegate to another identity.

3. Click ⋮ (**Actions**) > **Delegate approval**.

4. In the **Delegate approval**, in the **Delegate to** menu, select the identity to which you want to delegate the approval.

5. In the **Reason for your decision** field, enter a reason for the delegation.

6. Click **Save**.

Related topics

- Withdrawing delegations from pending requests on page 94

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 **Requests** > **Request History**.

2. On the **Request History** page, click **Details** next to the request with the approval delegation you want to withdraw.

3. In the **View Request Details** pane, click **Withdraw delegation**.

4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegation.

5. Click **Save**.

To withdraw multiple delegations from approvals

1. In the menu bar, click **Requests** > **Request History**.

2. On the **Request History** page, in the list, select the check boxes next to the requests whose approval delegations you want to withdraw.

3. Click ⋮ (**Actions**) > **Withdraw delegation**.

4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegations.

5. Click **Save**.

Related topics

- Delegating approvals of pending requests to other identities on page 93

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 **Requests** > **Pending requests**.

2. On the **Pending Requests** page, click **Details** next to the request that you do not want to make an approval decision about.

3. In the **View Request Details** pane, click **Reject approval**.

4. In the **Reject Approval**, in the **Reason for your decision** pane, enter a reason for the rejecting.

5. Click **Save**.

To reject approval of multiple requests

1. In the menu bar, click **Requests** > **Pending requests**.

2. On the **Pending Requests** page, in the list, select the check boxes next to the requests that you do not want to make an approval decision about.

3. Click ⋮ (**Actions**) > **Reject approval**.

4. In the **Reject Approval**, in the **Reason for your decision** pane, enter a reason for the rejecting.

5. Click **Save**.

   - Appointing additional approvers to pending requests on page 91

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.

To display the request history

1. In the menu bar, click **Requests** > **Request History**.

   This opens the **Request History** page.

2. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see Filtering on page 22). For example, this allows you to show just pending requests (no approval decision yet made).

3. (Optional) To display details of a request, click **Details** next to the request whose details you want to see.

Related topics

   - Canceling requests on page 95
   - Renewing products with limit validity periods on page 96
   - Unsubscribing products on page 98

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.

To cancel a request

1. In the menu bar, click **Requests** > **Request History**.

2. On the **Request History** page, click ▼ (**Filter**).

3. In the filter context menu, check the **Pending** box.

4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see Filtering on page 22). For example, this allows you to show just requests that you have carried out for other identities.

5. (Optional) If you want to cancel a request of another identity, in the 🔍 **Search** field, enter the identity's name.

6. Click **Details** next to the request you want to cancel.

7. In the **View Request Details** pane, click **Cancel request**.

8. In the **Cancel Request** pane, perform the following actions:

    a. In the **Reason for your decision** field, enter a reason for the cancellation.

    b. Click **Save**.

Related topics

- Requesting products on page 61
- Displaying request history on page 95
- Renewing products with limit validity periods on page 96
- Unsubscribing products on page 98

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 **Requests** > **Request History**.

2. On the **Request History** page, click ▼ (**Filter**).

3. In the filter context menu, check the **Active** box.

4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see Filtering on page 22). For example, this allows you to show just requests that you have carried out for other identities.

5. (Optional) If you want to renew a product of another identity, in the 🔍 **Search** field, enter the identity's name.

6. Next to the product that you want to renew, click **Details**.

7. In the **View Request Details** pane, click **Renew product**.

8. In the **Renew Product** pane, perform the following actions:

   a. In the **Renewal date** field, enter the renewal date for the product. If the field is empty the product has unlimited availability.

   b. In the **Reason for your decision** field, enter a reason for the renewal.

   c. Click **Save**.

To renew the validity period of multiple products

1. In the menu bar, click **Requests** > **Request History**.

2. On the **Request History** page, click ▼ (**Filter**).

3. In the filter context menu, check the **Active** box.

4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see Filtering on page 22). For example, this allows you to show just requests that you have carried out for other identities.

5. (Optional) If you want to renew products of another identity, in the 🔍 **Search** field, enter the identity's name.

6. Select the check boxes next to the products you want to renew.

7. Click ⋮ (**Actions**) > **Renew product**.

8. In the **Renew Product** pane, perform the following actions:

   a. In the **Renewal date** field, enter the renewal date for the products. If the field is empty the products have unlimited availability.

   b. In the **Reason for your decision** field, enter a reason for the renewal.

   c. Click **Save**.

Related topics

- Setting the validity period of products in your shopping cart on page 65
- Canceling requests on page 95
- Unsubscribing products on page 98

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 **Requests** > **Request History**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, check the **Active** box.
4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see Filtering on page 22). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to unsubscribe a product of another identity, in the 🔍 **Search** field, enter the identity's name.
6. In the list, click **Details** next to the product that you want to unsubscribe.
7. In the **View Request Details** pane, click **Unsubscribe product**.
8. In the **Unsubscribe Product** pane, perform the following actions:
   a. 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**.
   b. In the **Reason for your decision** field, enter a reason for unsubscribing.
   c. In the **Additional comments about your decision** field, enter extra information about unsubscribing.
   d. Click **Save**.

To unsubscribe multiple products

1. In the menu bar, click **Requests** > **Request History**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, check the **Active** box.
4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see Filtering on page 22). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to unsubscribe products of another identity, in the 🔍 **Search** field, enter the identity's name.
6. In the list, select the check boxes next to the products you want to unsubscribe.
7. Click ⋮ (**Actions**) > **Unsubscribe product**.
8. In the **Unsubscribe Product** pane, perform the following actions:

a. In the **Unsubscribed as from** field, enter the date for unsubscribing the products. If you leave this field empty, the products are unsubscribed once you have clicked **Saved**.

b. In the **Reason for your decision** field, enter a reason for unsubscribing.

c. In the **Additional comments about your decision** field, enter extra information about unsubscribing.

d. Click **Save**.

Related topics

- Displaying request history on page 95
- Renewing products with limit validity periods on page 96
- Canceling requests on page 95

Displaying approvals

You can display all approvals of product requests that you decided upon.

To display approvals

1. In the menu bar, click **Requests** > **Request History**.

2. On the **Request History** page, click ▼ (**Filter**).

3. In the filter context menu, check the **My approvals** box.

4. (Optional) To display request details (for example, the approval workflow or who can make approval decisions about the request), click **Details** next to the request.

Related topics

- Withdrawing delegations from pending requests on page 94
- Removing additional approvers of pending requests on page 92
- Approving and denying requests on page 86
- Undoing approvals on page 99

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 **Requests** > **Request History**.

2. (Optional) To control which requests are displayed on the **Request History** page, click ▼ (**Filter**) (see Filtering on page 22). For example, this allows you to show just pending requests (no approval decision yet made).

3. In the list, click **Details** next to the request whose the approval that you want to undo.

4. In the **View Request Details** pane, click **Undo approval decision**.

5. In the **Undo Approval Decision** dialog, perform the following actions:

   a. In the **Reason for your decision**, enter why you want to undo the approval.

   b. Click **Save**.

Related topics

- Displaying approvals on page 99

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

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.

Detailed information about this topic

- Attestation policies on page 102
- Starting attestation on page 112
- Running sample attestations on page 113
- Attestation runs on page 114
- Attestation by peer group analysis on page 117
- Managing samples on page 117

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 102
- Setting up attestation policies on page 104
- Editing attestation policies on page 106
- Copying attestation policies on page 109
- Deleting attestation policies on page 112
- Appendix: Attestation conditions and approval policies from attestation procedures on page 290

Displaying attestation policies

You can display enabled and disabled attestation policies.

To display attestation polices

1. In the menu bar, click **Attestation** > **Attestation Policies**.

   This opens the **Attestation Policies** page.

2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click ✖ next to the filter (**Clear filter**).

3. (Optional) To display more details of an attestation policy, click **Details** next to the attestation policy.

Related topics

- Displaying attestation policies main data on page 103

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** > **Attestation Policies**.

2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click ⊗ next to the filter (**Clear filter**).

3. Next to the attestation policy whose main data you want to show, click **Edit**.

   This opens the **Attestation Policy Settings** pane.

4. (Optional) To display the objects that fulfill the conditions, perform one of the following actions:

   - Objects that fulfill one condition: Under **Objects To Be Attested by This Attestation Policy**, click the number link next to the condition.

   - Objects that fulfill all conditions: Next to **Objects To Be Attested by This Attestation Policy**, click the number link.

Displaying attestation policy reports

You can the display reports of attestation policies. These reports contain detailed information about attestation policies.

To display an attestation policy's report

1. In the menu bar, click **Attestation** > **Attestation Policies**.

2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click ⊗ next to the filter (**Clear filter**).

3. On the **Attestation Policies** page, click ⋮ (**Actions**) > **Download report** next to the attestation policy whose report you want to display.

   Once the report is completely downloaded, you can open it.

Related topics

- Displaying attestation run reports on page 116

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** > **Attestation Policies**.
2. On the **Attestation Policies** page, click **Create attestation policy**.
3. In the **Create Attestation Policy** pane, enter the new attestation policy's main data.

Table 17: 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	Select which objects to attest 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

Property	Description
	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.
Sample	Select which sampling data you want to use (see Running sample attestations on page 113). NOTE: You can only select samples that have not yet been assigned to an attestation policy. NOTE: When you select samples, you can not set conditions anymore and vice versa.
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.

4. To specify which objects to attest, under **Objects To Be Attested by This Attestation Policy**, click **Add condition**.

5. In the **Condition type** menu, click the condition type to use (see Appendix: Attestation conditions and approval policies from attestation procedures on page 290).

   NOTE: The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.

ONE IDENTITY
by Quest

6. (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 290).

7. (Optional) Create more conditions if required. To do this, click **Add another condition**.

8. (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.

9. Click **Create**.

Related topics

- Appendix: Attestation conditions and approval policies from attestation procedures on page 290

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** > **Attestation Policies**.

2. On the **Attestation Policies** page, next to the attestation policy you want to edit, click **Edit**.

   To view disabled attestation policies, clear the **Activated attestation policies only** filter. To do this, click ⊗ next to the filter (**Clear filter**).

   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 109).

3. In the **Edit Attestation Policy** pane, edit the attestation policy's main data.

Table 18: 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	Select which objects to attest 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

Property	Description
	regulatory requirements. For example, internal requirements or auditing requirements.
Sample	Select which sampling data you want to use (see Running sample attestations on page 113). NOTE: You can only select samples that have not yet been assigned to an attestation policy. NOTE: When you select samples, you can not set conditions anymore and vice versa.
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.

4. To specify which objects to attest, perform one of the following actions:

    - To add a new condition, under **Objects To Be Attested by This Attestation Policy** click **Add another condition**.

    - To edit an existing condition, under **Objects To Be Attested by This Attestation Policy**, click the condition.

    - To delete an existing condition, click 🗑 (**Delete condition**).

5. In the **Condition type** menu, click the condition type to use (see Appendix: Attestation conditions and approval policies from attestation procedures on page 290).

    NOTE: The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.

6. (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 290).

7. (Optional) Create or modify more conditions if required. To do this, click **Add another condition**.

8. (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.

9. Click **Save**.

Related topics

- Appendix: Attestation conditions and approval policies from attestation procedures on page 290

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** > **Attestation Policies**.

2. On the **Attestation Policies** page, next to the attestation policy you want to copy, click ⋮ (**Actions**) > **Copy**.

   To view disabled attestation policies, clear the **Activated attestation policies only** filter. To do this, click ⊗ next to the filter (**Clear filter**).

3. In the **Copy Attestation Policy** pane, edit the attestation policy's main data.

   Table 19: 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.

Property	Description
Description	Enter a description of the attestation policy.
Attestation procedure	Select which objects to attest 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.
Sample	Select which sampling data you want to use (see Running sample attestations on page 113). NOTE: You can only select samples that have not yet been assigned to an attestation policy. NOTE: When you select samples, you can not set conditions

Property	Description
	anymore and vice versa.
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.

4. To specify which objects to attest, perform one of the following actions:

   - To add a new condition, under **Objects To Be Attested by This Attestation Policy** click **Add another condition**.

   - To edit an existing condition, under **Objects To Be Attested by This Attestation Policy**, click the condition.

   - To delete an existing condition, click 🗑 (**Delete condition**).

5. In the **Condition type** menu, click the condition type to use (see Appendix: Attestation conditions and approval policies from attestation procedures on page 290).

   NOTE: The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.

6. (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 290).

7. (Optional) Create or modify more conditions if required. To do this, click **Add another condition**.

8. (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.

9. Click **Create**.

Related topics

- Appendix: Attestation conditions and approval policies from attestation procedures on page 290

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** > **Attestation Policies**.

2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click ⊗ next to the filter (**Clear filter**).

3. On the **Manage Attestation Policies** page, click ⋮ (**Actions**) > **Delete** next to the attestation policy you want to delete.

4. In the **Delete attestation policy** dialog, confirm the prompt with **Yes**.

Starting attestation

In the Web Portal, there are two ways for you to set up attestation cases for an attestation policy. You can trigger attestation through a scheduled task or you can start selected objects individually.

NOTE: You cannot start attestation with attestation policies in the **In Processing** state.

To start attestation using a scheduled task

1. In the menu bar, click **Attestation** > **Attestation Policies**.

2. On the **Attestation Policies** page, click **Edit** next to the attestation policy you want attest.

   TIP: To display disabled attestation policies, enable the **Show disabled policies**.

3. In the **Edit attestation policy** pane, deselect the **Disabled** box.

4. In the **Calculation schedule** menu, specify how often an attestation run with this attestation policy is started.

   Each attestation run creates a new attestation case respectively.

5. Click **Save**.

To start attestation for selected objects

1. In the menu bar, click **Attestation** > **Attestation Policies**.

2. On the **Attestation Policies** page, next to the attestation policy that you want to start, click ⋮ (**Actions**) > **Start attestation**.

3. In the **Start attestation** pane, perform one of the following actions:

   - To start attesting an object, click **Start attestation** next to the object.

   - To start attesting several object, select the check box in front of each object and click **Start attestation for selected**.

   - To start attesting all objects, click **Start attestation for all**.

Related topics

- Editing attestation policies on page 106
- Running sample attestations on page 113

Running sample attestations

You can perform attestations only for a subset of identities. For example, when attesting all identities would take too long. Samples contains identities that you can use to conduct such sample attestation.

To use sample data in an attestation, assign a sample to the corresponding attestation policy and start the attestation.

To run a sample attestation

1. In the menu bar, click **Attestation** > **Attestation Policies**.

2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click ✖ next to the filter (**Clear filter**).

3. Next to the attestation policy you want to use for the sample attestation, click **Edit**.

4. In the details pane, in the **Sample** menu, select the sample you want to use.

5. Click **Save**.

   NOTE: If the attestation policy is enabled and a schedule is set up, the sample attestation is automatically carried out on the selected date and you do not need to take any further action.

6. On the **Attestation Policies** page, click ⋮ (**Actions**) > **Start attestation** next to the attestation policy you want to use for the sample attestation.

7. In the **Start attestation** pane, perform one of the following actions:

   - To start attesting an object, click **Start attestation** next to the object.
   - To start attesting several objects, select the check box in front of each object and click **Start attestation for selected**.
   - To start attesting all objects, click **Start attestation for all**.

Related topics

- Managing samples on page 117

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 114
- Displaying attestors of application runs on page 115
- Displaying attestation cases of application runs on page 115
- Displaying attestation run reports on page 116
- Extending attestation runs on page 116
- Sending reminders about attestation runs on page 119

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** > **Attestation runs**.

   This opens the **Attestation Policy Runs** page

2. (Optional) To view more details (current data, attestation details, and attestation prediction) of an attestation run, next to the attestation run, click **Details** and take the relevant information from the **View Attestation Run Details** pane on the **Details** tab.

Related topics

Displaying attestors of application runs

You can show all the attestors that still need to make approval decisions about attestation cases in an attestation run.

In addition, you can send reminders to these attestors (see).

To show attestors 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 whose attestor you want to display.

3. In the **View Attestation Run Details** pane, click the **Attestors** tab.

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 120
- Granting or denying attestation cases on page 121

Displaying attestation run reports

You can the display reports of attestation runs. These reports contain detailed information about the attestation runs.

To display an attestation run's report

1. In the menu bar, click **Attestation** > **Attestation runs**.
2. On the **Attestation Runs** page, click **Details** next to the attestation run whose report you want to display.
3. In the **View Attestation Run Details** pane, click **Download report**.

   Once the report is completely downloaded, you can open it.

Related topics

- Displaying attestation policy reports on page 103

Extending attestation runs

You can extend attestation runs.

To extend an attestation run

1. In the menu bar, click **Attestation** > **Attestation runs**.
2. On the **Attestation Policy Runs** page, click **Details** next to the attestation run that you want to extend.
3. In the **View Attestation Run Details** pane, click **Extend attestation run**.
4. In the **Extend attestation run** pane, in the **New due date** field, enter a new due date.
5. In the **Reason** field, enter a reason for extending.
6. Click **Extend attestation run**.

Related topics

- Sending reminders about attestation runs on page 119

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 290

Managing samples

You can perform attestations only for a subset of identities. For example, when attesting all identities would take too long. Samples contains identities that you can use to conduct such sample attestation.

TIP: To use samples in an attestation, assign a sample to the corresponding attestation policy and start the attestation (see Running sample attestations on page 113).

Detailed information about this topic

- Displaying samples on page 117
- Creating samples on page 118
- Editing samples on page 118
- Deleting samples on page 119

Displaying samples

You can display all existing samples.

To display samples

1. In the menu bar, click **Attestation** > **Sample data**.

   This opens the **Sample Data** page.

2. (Optional) To view a sample's data, click **Edit** next to the sample.

Creating samples

You can create new samples. To do this, you create a sample and assign the corresponding sample data to it.

To create a sample

1. In the menu bar, click **Attestation** > **Sample data**.

2. On the **Sample Data** page, click **Create sample**.

3. In the **Create sample** pane, enter the name of the sample in the **Display name** field.

4. Click **Continue**.

5. In the **Assign identities** step, select the check box in front of the identity to which you want to assign the sample.

   TIP: To create an empty sample, do not select a check box and click **Skip**. You can assign identities to the sample later by editing it.

6. Click **Continue**.

7. In the **Summary** step, click **Save**.

Editing samples

You can assign additional identities to existing samples or remove them.

To assign another identity to a sample

1. In the menu bar, click **Attestation** > **Sample data**.

2. On the **Sample Data** page, click **Edit** next to the sample you want to edit.

3. In the **Edit Sample** pane, click **Assign identities**.

4. In the **Select Identities** pane, select the check box next to the identity you want to assign to the samples.

5. Click **Assign**.

To remove an identity from a sample

1. In the menu bar, click **Attestation** > **Sample data**.

2. On the **Sample Data** page, click **Edit** next to the sample you want to edit.

3. In the **Edit Sample** pane, select the check box next to the identity you want to remove.

4. Click **Remove identities**.

5. In the **Remove Identities** dialog, confirm the prompt with **Yes**.

Deleting samples

You can delete existing samples.

To delete a sample

1. In the menu bar, click **Attestation** > **Sample data**.

2. On the **Sample Data** page, select the check box next to the sample you want to delete.

   TIP: To delete multiple samples, select additional check boxes in front of the respective samples.

3. Click **Delete**.

4. In the **Delete Sample** dialog box, confirm the prompt with **Yes**.

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 belong to certain attestation runs (see Sending reminders about attestation runs on page 119).

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** > **Attestation runs**.

2. On the **Attestation Policy Runs** page, click **Send reminders for displayed runs**.

3. (Optional) In the **Send Reminder** pane, in the **Message** field, enter the message for the attestor. This message is added to the reminder.

4. Click **Send reminder**.

To send a reminder to attestors of a selected attestation run

1. In the menu bar, click **Attestation** > **Attestation runs**.

2. On the **Attestation Policy Runs** page, click **Details** next to the attestation run that has the attestors you want to remind.

3. Perform one of the following actions:

   - To send a reminder to all attestors of the attestation run, in the **View Attestation Run Details** pane, click **Send reminder to all attestors**.

   - To send a reminder to specific attestors of the attestation run, in the **View Attestation Run Details** pane, click the **Attestors** tab, select the check boxes in front of the corresponding attestors and click **Send reminder**.

4. (Optional) In the **Send Reminder** pane, in the **Message** field, enter the message for the attestor. This message is added to the reminder.

5. Click **Send reminder**.

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 120
- Granting or denying attestation cases on page 121
- Appointing other approvers for pending attestation cases on page 122
- Rejecting approval of attestation cases on page 128

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** > **Pending Attestations**.

   This opens the **Pending Attestations** page.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

- To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

- To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. (Optional) To show more details of an attestation case, click **Details** next to the attestation case.

4. (Optional) To display objects involved in an attestation case in detail, perform the following actions:

   a. Next to the attestation case, click **Details**.

   b. In the **View Attestation Case Details** pane, click **Show details** or **Download report**.

5. (Optional) To display all the identities that can approve an attestation case, perform the following actions:

   a. Next to the attestation case, click **Details**.

   b. In the **View Attestation Case Details** pane, click the **Workflow** tab.

6. (Optional) To display compliance violations of an attestation case, perform the following actions:

   a. Next to the attestation case, click **Details**.

   b. In the **View Attestation Case Details** pane, click the **Compliance Violations** tab.

   c. (Optional) To edit mitigating controls for the attestation case, on the **Compliance Violations** tab, click **Edit mitigating controls** and assign an appropriate mitigating controls.

Related topics

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** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

- To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. (Optional) To approve an attestation case as a member of the chief approval team and only display the relevant attestation cases, toggle the **Show attestation cases to be approved by chief approval team** switch.

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 approve or deny multiple attestation cases, in the list, select the check boxes next to the attestation cases and click **Approve** or **Deny** below the list.

5. (Optional) In the **Approve Attestation Case**/**Deny Attestation Case** pane, perform the following actions:

   a. In the **Reason for your decision** field, select a standard reason for your approval decision.

   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

   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

- Displaying attestation cases of application runs on page 115

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 123).

- Appoint additional approver
  You can give an another identity the task of approving Appointing additional approvers to pending attestation cases on page 124). 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 128).
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 126). 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 128).
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** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

   - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, click **Details** next to the attestation case whose approval you want to reroute.

4. In the **View Attestation Case Details** pane, click **Reroute approval**.

5. In the **Reroute approval** pane, in the **Select approval level** menu, select the approval level you want to reroute to.

6. (Optional) In the **Reason for your decision** field, enter a reason for rerouting.

7. Click **Save**.

To reroute multiple approvals

1. In the menu bar, click **Attestation** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

- To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases whose approvals you want to reroute.

4. Click ⋮ (**Actions**) > **Reroute approval**.

5. In the **Reroute Approval** pane, in the **Select approval level** menu, select the respective approval level to reroute to.

6. (Optional) In the **Reason for your decision** field, enter a reason for rerouting.

7. Click **Save**.

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** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

    - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

    - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, in the list, click **Details** next to the attestation case to which you want to add an additional approver.

4. In the **View Attestation Case Details** pane, click **Add attestor**.

5. In the **Add Additional Attestor** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.

6. In the **Reason for your decision** field, select a standard reason for adding an additional approver.

7. Click **Save**.

To add an additional approver to multiple attestation cases

1. In the menu bar, click **Attestation** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

    - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

- To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases to which you want to add an additional approver.

4. Click ⋮ (**Actions**) > **Add attestor**.

5. In the **Add Additional Attestor** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.

6. In the **Reason for your decision** field, select a standard reason for adding an additional approver.

7. Click **Save**.

Related topics

- Removing additional approvers from pending attestation cases on page 125

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.

To withdraw an attestation case's additional approver

1. In the menu bar, click **Attestation** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

   - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, click **Details** next to the attestation case to which you added an additional approver.

4. In the **View Attestation Case Details** pane, click **Withdraw additional attestor**.

5. In the **Withdraw Additional Attestor** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.

6. Click **Save**.

To withdraw an additional approver from multiple attestation cases

1. In the menu bar, click **Attestation** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

   - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases to which you added an additional approver.

4. Click ⋮ (**Actions**) > **Withdraw additional attestor**.

5. In the **Withdraw Additional Attestor** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.

6. Click **Save**.

Related topics

- Appointing additional approvers to pending attestation cases on page 124

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 127).

To delegate an approval

1. In the menu bar, click **Attestation** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

   - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, click **Details** next to the attestation case whose approval decision you want to delegate to another identity.

4. In the **View Attestation Case Details** pane, click **Delegate approval**.

5. In the **Delegate approval**, in the **Delegate to** menu, select the identity to which you want to delegate the approval.

6. In the **Reason for your decision** field, enter a reason for the delegation.

7. Click **Save**.

To delegate approval of multiple attestation cases

1. In the menu bar, click **Attestation** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

   - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases whose approval you want to delegate to another identity.

4. Click ⋮ (**Actions**) > **Delegate approval**.

5. In the **Delegate approval**, in the **Delegate to** menu, select the identity to which you want to delegate the approval.

6. In the **Reason for your decision** field, enter a reason for the delegation.

7. Click **Save**.

Related topics

- Withdrawing delegations from pending attestation case approvals on page 127

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** > **Attestation history**.

2. On the **Attestation History** page, click **Details** next to the request whose approval delegation you want to withdraw.

3. In the **View Attestation Case Details** pane, click **Withdraw delegation**.

4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegation.

5. Click **Save**.

To withdraw multiple delegations from approvals

1. In the menu bar, click **Attestation** > **Attestation history**.

2. On the **Attestation History** page, in the list, select the check boxes next to the attestation cases whose approval delegations you want to withdraw.

3. Click ⋮ (**Actions**) > **Withdraw delegation**.

4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegations.

5. Click **Save**.

Related topics

- Delegating approvals of pending attestation cases to other identities on page 126

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** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

   - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, click **Details** next to the attestation case that you do not want to make an approval decision about.

4. In the **View Attestation Case Details** pane, click **Reject approval**.

5. In the **Reject Approval**, in the **Reason for your decision** pane, enter a reason for the rejecting.

6. Click **Save**.

To reject approval of multiple attestation cases

1. In the menu bar, click **Attestation** > **Pending Attestations**.

2. (Optional) On the **Pending attestations** page, perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

- To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.

3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases that you do not want to make an approval decision about.

4. Click ⋮ (**Actions**) > **Reject approval**.

5. In the **Reject Approval**, in the **Reason for your decision** pane, enter a reason for the rejecting.

6. Click **Save**.

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** > **Attestation history**.

   This opens the **Attestation History** page.

2. Perform one of the following actions:

   - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.

   - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Attestation policy**.

3. (Optional) To control which attestation cases are displayed, click ▼ (**Filter**) (see Filtering on page 22). 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 **Details** next to the attestation case whose details you want to display.

Related topics

- Withdrawing delegations from pending attestation case approvals on page 127

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

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** > **Compliance rules**.

   This opens the **Compliance rules** page.

2. (Optional) To further limit or extend which compliance rules are displayed, click ▼ (**Filter**) and in the context menu, under **Status**, select one of the following filters:

   - **Activated**: Select this filter to display only enabled compliance rules.

   - **Deactivated**: Select this filter to display only disabled compliance rules.

   TIP: To view all compliance rules, clear the filter. To do this, click **Clear filters** on the context menu.

3. (Optional) To view more details of a compliance rule, click **Details** next to the compliance rule.

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** > **Compliance rules**.

2. (Optional) To further limit or extend which compliance rules are displayed, on the **Compliance Rules** page, click ▼ (**Filter**) and in the context menu, under **Status**, select one of the following filters:

   - **Activated**: Select this filter to display only enabled compliance rules.

   - **Deactivated**: Select this filter to display only disabled compliance rules.

   TIP: To view all compliance rules, clear the filter. To do this, click **Clear filters** on the context menu.

3. Click **Details** next to the compliance rule whose report you want to see.

4. In the **View Compliance Rule Details** pane, click **Download report**.

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

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** > **Rule violations**.

   This opens the **Rule Violations** page opens and displays all the rule violations that are still subject to approval.

2. (Optional) To display rule violations that have already been approved or denied, click ▼ (**Filter**) and enable the corresponding option in the menu.

3. (Optional) To display a rule violation, next to the rule violation, click **Details**.

Related topics

- Regelverletzungen meiner Identitäten anzeigen
- Alle Regelverletzungen anzeigen
- Entscheidbare Richtlinienverletzungen anzeigen
- Meine Aufgaben
- Offene Regelverletzungen

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** > **Rule violations**.

2. On the **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**.

TIP: To grant or deny exceptions to several rule violations at the same time, select the check box next to each rule violation and click **Grant exception** or **Deny exception** at the bottom of the list.

3. (Optional) To set an approval deadline, in the **Grant exception**/**Deny exception** pane, in the **Valid until** field, enter a date and time.

4. (Optional) Perform the following actions:

   a. In the **Reason for your decision** menu, select a standard reason for your approval decision.

   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

   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.

5. Click **Save**.

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 134
- Delegating tasks on page 210
- Ownerships on page 213

My responsibilities

You can manage objects that you are responsible for within your company. Possible objects are:

- Identities
- Hierarchical roles
    - Organizations
        - Departments
        - Cost centers
        - Locations
    - Business roles
- Company resources
    - System entitlements

Detailed information about this topic

- Managing my identities on page 159
- Managing my system entitlements on page 192

ONE IDENTITY
by Quest

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

You can display all the departments for which you are responsible.

To display departments

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

   This opens the **Departments** page and displays all the departments for which you are responsible.
3. (Optional) To display details of a department, next to the department, click **Edit**.

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department whose main data you want to show/edit, click **Edit**.

4. In the **Edit Department** pane, make your changes in the corresponding fields.

You can edit the following main data.

Table 20: 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	Select the manager who is responsible for the department.
2nd Manager	Select an identity to act as a deputy to the department's manager.
Additional manager	Click **Assign**/**Change** and select a cost center. Members of the selected application role are responsible for the department.
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.

5. Click **Save**.

Copying/splitting my departments

You can copy or move memberships and entitlements from departments you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a department or move memberships and entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department you want to copy or whose memberships and entitlements you want to move, click **Edit**.

4. In the **Edit Department** pane, click ⋮ (**Actions**) > **Split**.

5. In the **Split** pane, In the **Type of new role** menu, select which type to give the new object.

6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

   TIP: After the object has been created, you can add the remaining main data (see Displaying and editing my department main data on page 135, Displaying and editing my business roles' main data on page 151, Displaying and editing my cost center main data on page 176, or Displaying and editing my locations' main data on page 184).

7. Click **Continue**.

8. In the **Select assignments to be copied or moved to the new role** step, perform the following actions:

   - To neither copy nor move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep this assignment**. The entitlement/membership is later only available in the source object.

   - To copy or move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new role**. The entitlement/membership is included later in the source object as well as the target object.

   - To move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new role**. The entitlement/membership is later removed from the source object and only included in the target object.

9. Click **Continue**.

10. (Optional) In the **Verify** step, you verify the actions to run and deselect the check box in front of any actions that should not be run.

11. Click **Continue**.

Related topics

- Managing my department memberships on page 139
- Managing my departments' entitlements on page 142

Managing my department memberships

As soon as an identity is assigned to a department, the identity becomes a member in the department.

Detailed information about this topic

Displaying memberships in my departments

You can display identities that are assigned departments for which you are responsible.

To display identities that are assigned a department

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Departments**.
3. On the **Departments** page, next to the department whose memberships you want to display, click **Edit**.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To display all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my departments

You can see how a department assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Departments**.
3. On the **Departments** page, next to the department whose memberships you want to display, click **Edit**.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

Adding identities to my departments

You can assign identities to departments for which you are responsible.

The following assignment options are available:

- Assignment by request
- Automatic assignment through a dynamic role
- Revoking exclusion of a member

To assign an identity to a department using a request

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department you want to add an identity to, click **Edit**.

4. In the **Edit Department** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Click **Request memberships**.

7. In the **Select Identities** pane, select the check box next to the identity you want to assign to the department.

8. Click **Request memberships**.

9. Close the **Edit Department** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the department.

To add members automatically through a dynamic role

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department for which you want to create a dynamic role, click **Edit**.

4. In the **Edit Department** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.

6. Click **Create dynamic role**.

7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:

a. In the **Property** menu, select the relevant property.

b. In the **Operator** menu, select a logical operator.

c. In the final field, specify a comparison value.

d. (Optional) To add another condition, click **Add another condition** and repeat the steps.

e. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

TIP: To remove a condition, click 🗑 (**Delete**).

For more information about customizing filter conditions, see Custom filter conditions.

8. Click **Save**.

9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.

10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.

11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department you want to add again, click **Edit**.

4. In the **Edit Department** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.

7. Click **Remove exclusion**.

Related topics

- Requesting products on page 61

Removing identities from my departments

You can remove departments from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a department from an identity

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department with a membership you want to delete, click **Edit**.

4. In the **Edit Department** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

9. If the member was assigned through a dynamic role, perform the following actions:

   a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.

   b. Click **Exclude members**.

Managing my departments' 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 142
- Adding entitlements to my departments on page 143
- Deleting my department entitlements on page 143

Displaying my department entitlements

You can display entitlements that are assigned departments for which you are responsible.

To display entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department whose entitlements you want to display, click **Edit**.

4. In the **Edit Department** pane, click the **Permissions** tab.

Adding entitlements to my departments

You can add entitlements to departments for which you are responsible. You do this through requests.

To add an entitlement to a department

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department you want to add an entitlement to, click **Edit**.

4. In the **Edit Department** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, click **Request entitlements**.

6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.

7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.

9. Close the **Edit Department** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    After the request has been granted approval, the entitlement is added to the department.

Related topics

- Requesting products on page 61

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department whose entitlement you want to delete, click **Edit**.

4. In the **Edit Department** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.

6. Click **Remove**.

7. Confirm the prompt with **Yes** in the dialog.

Displaying my departments' rule violations

You can see the rule violations of departments for which you are responsible.

To display rule violations

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Departments**.

3. On the **Departments** page, next to the department whose rule violations you want to display, click **Edit**.

4. On the **Edit Department** pane, click the **Rule Violations** tab.

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

You can display all the application roles for which you are responsible.

To display application roles

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Application roles**.

   This opens the **Application Roles** page and displays all the application roles for which you are responsible.

3. (Optional) To display details of an application role, next to the application role, click **Edit**.

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. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Application roles**.
3. On the **Application Roles** page, next to the application role whose main data you want to show/edit, click **Edit**.
4. In the **Edit Application role** pane, make your changes in the corresponding fields.

You can edit the following main data.

Table 21: 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.
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.

5. Click **Save**.

Managing my application role memberships

As soon as an identity is assigned to an application role, the identity becomes a member in the application role.

Detailed information about this topic

Displaying memberships in my application roles

You can display identities that are assigned application roles for which you are responsible.

To display identities that are assigned an application role

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Application roles**.

3. On the **Application Roles** page, next to the application role whose memberships you want to display, click **Edit**.

4. In the **Edit Application role** pane, click the **Memberships** tab.

5. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my application roles

You can see how an application role assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Application roles**.

3. On the **Application Roles** page, next to the application role whose memberships you want to display, click **Edit**.

4. In the **Edit Application role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

Assigning identities to my application roles

You can assign identities to application roles for which you are responsible.

The following assignment options are available:

- Assignment by request

- Automatic assignment through a dynamic role

- Revoking exclusion of a member

To assign an identity to a application role using a request

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Application roles**.

3. On the **Application Roles** page, next to the application role you want to add an identity to, click **Edit**.

4. In the **Edit Application Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Request memberships**.

6. In the **Select Identities** pane, select the check box next to the identity you want to assign to the application role.

7. Click **Request memberships**.

8. Close the **Edit Application Role** pane.

9. In the menu bar, click **Requests** > **Shopping cart**.

10. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the application role.

To add members automatically through a dynamic role

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Application roles**.

3. On the **Application Roles** page, next to the application role for which you want to create a dynamic role, click **Edit**.

4. In the **Edit Application Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.

6. Click **Create dynamic role**.

7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:

   a. In the **Property** menu, select the relevant property.

   b. In the **Operator** menu, select a logical operator.

   c. In the final field, specify a comparison value.

   d. (Optional) To add another condition, click **Add another condition** and repeat the steps.

   e. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

   | TIP: To remove a condition, click 🗑 (**Delete**).

   For more information about customizing filter conditions, see Custom filter conditions.

8. Click **Save**.

9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.

10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.

11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Application roles**.

3. On the **Application Roles** page, next to the application role you want to add again, click **Edit**.

4. In the **Edit Application Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.

7. Click **Remove exclusion**.

Related topics

- Requesting products on page 61

Removing identities from my application roles

You can remove application roles from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove an application role from an identity

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Application roles**.

3. On the **Application Roles** page, next to the application role with a membership you want to delete, click **Edit**.

4. In the **Edit Application Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

9. If the member was assigned through a dynamic role, perform the following actions:

a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.

b. Click **Exclude members**.

Displaying my application roles' rule violations

You can see the rule violations of application roles for which you are responsible.

To display rule violations

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Application roles**.

3. On the **Application Roles** page, next to the application role whose rule violations you want to display, click **Edit**.

4. On the **Edit Application Role** pane, click the **Rule Violations** tab.

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

You can display all the business roles for which you are responsible.

To display business roles

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

   This opens the **Business Roles** page and display all the business roles for which you are responsible.

3. (Optional) To display details of a business role, next to the business role, click **Edit**.

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role whose main data you want to show/edit, click **Edit**.

4. In the **Edit Business Role** pane, make your changes in the corresponding fields.

You can edit the following main data.

Table 22: 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	Select the manager who is responsible for the business role.
2nd Manager	Select an identity to act as a deputy to the business role's manager.
Additional manager	Click **Assign**/**Change** and select a cost center. Members of the selected application role are responsible for the department.
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.

5. Click **Save**.

Copying/splitting my business roles

You can copy or move memberships and entitlements from business roles you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a business role or move memberships and entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role you want to copy or whose memberships and entitlements you want to move, click **Edit**.

4. In the **Edit Business Role** pane, click ⋮ (**Actions**) > **Split**.

5. In the **Split** pane, In the **Type of new role** menu, select which type to give the new object.

6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

   TIP: After the object has been created, you can add the remaining main data (see Displaying and editing my department main data on page 135, Displaying and editing my business roles' main data on page 151, Displaying and editing my cost center main data on page 176, or Displaying and editing my locations' main data on page 184).

7. Click **Continue**.

8. In the **Select assignments to be copied or moved to the new role** step, perform the following actions:

   • To neither copy nor move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep this assignment**. The entitlement/membership is later only available in the source object.

   • To copy or move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new role**. The entitlement/membership is included later in the source object as well as the target object.

   • To move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new role**. The entitlement/membership is later removed from the source object and only included in the target object.

9. Click **Continue**.

10. (Optional) In the **Verify** step, you verify the actions to run and deselect the check box in front of any actions that should not be run.

11. Click **Continue**.

Related topics

Managing my business role memberships

As soon as a business role is assigned to an identity, the identity becomes a member in the business role.

Detailed information about this topic

Displaying my business roles' memberships

You can display identities that are assigned business roles for which you are responsible.

To display identities that are assigned a business role

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.
3. On the **Business Roles** page, next to the business role whose memberships you want to display, click **Edit**.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To display all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my business roles

You can see how a business role under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role whose memberships you want to display, click **Edit**.

4. In the **Edit Business Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

Assigning identities to my business roles

You can assign identities to business roles for which you are responsible.

The following assignment options are available:

- Assignment by request
- Automatic assignment through a dynamic role
- Revoking exclusion of a member

To assign an identity to a business role using a request

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role you want to add an identity to, click **Edit**.

4. In the **Edit Business Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Click **Request memberships**.

7. In the **Select Identities** pane, select the check box next to the identity you want to assign to the business role.

8. Click **Request memberships**.

9. Close the **Edit Business Roles** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the business role.

To add members automatically through a dynamic role

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role for which you want to create a dynamic role, click **Edit**.

4. In the **Edit Business Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.

6. Click **Create dynamic role**.

7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:

    a. In the **Property** menu, select the relevant property.

    b. In the **Operator** menu, select a logical operator.

    c. In the final field, specify a comparison value.

    d. (Optional) To add another condition, click **Add another condition** and repeat the steps.

    e. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

    TIP: To remove a condition, click 🗑 (**Delete**).

    For more information about customizing filter conditions, see Custom filter conditions.

8. Click **Save**.

9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.

10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.

11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role you want to add again, click **Edit**.

4. In the **Edit Business Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.

7. Click **Remove exclusion**.

Related topics

- Requesting products on page 61

Removing identities from my business roles

You can remove business roles from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a business role from an identity

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role with a membership you want to delete, click **Edit**.

4. In the **Edit Business Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

9. If the member was assigned through a dynamic role, perform the following actions:

   a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.

   b. Click **Exclude members**.

Managing 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 157
- Adding entitlements to my business roles on page 158
- Deleting my business roles' entitlements on page 158

Displaying my business roles' entitlements

You can display entitlements that are assigned business roles for which you are responsible.

To display entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role whose entitlements you want to display, click **Edit**.

4. In the **Edit Business Role** pane, click the **Permissions** tab.

Adding entitlements to my business roles

You can add entitlements to business roles for which you are responsible. You do this through requests.

To add an entitlement to a business role

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role you want to add an entitlement to, click **Edit**.

4. In the **Edit Business Role** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, click **Request entitlements**.

6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.

7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.

9. Close the **Edit Business Role** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    After the request has been granted approval, the entitlement is added to the business role.

Related topics

- Requesting products on page 61

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.

3. On the **Business Roles** page, next to the business role whose entitlement you want to delete, click **Edit**.

4. In the **Edit Business Role** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.

6. Click **Remove**.

7. Confirm the prompt with **Yes** in the dialog.

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. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.
3. On the **Business Roles** page, next to the business role whose rule violations you want to display, click **Edit**.
4. On the **Edit Business Role** pane, click the **Rule Violations** tab.

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

- Displaying my identities on page 160
- Displaying and editing my identities' main data on page 160
- Adding your own identities on page 162
- Displaying my identities' risk indexes
- Deactivating my identities on page 166
- Reactivating my identities on page 166
- Marking my identities as security risks on page 166
- Revoking my identities' security risks on page 167
- Assigning other managers to my identities on page 167
- Creating passcodes for my identities on page 168
- Creating reports about my identities on page 169
- Managing my identities' memberships
- Displaying identities' organizational charts on page 173
- Displaying my identities' history on page 173
- Managing my identities' attestation cases on page 173
- Displaying my identities' rule violations on page 175

Displaying my identities

You can display all the identities for which you are responsible.

To display identities

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

   This opens the **Identities** page and displays all the identities that report directly to you.

3. (Optional) To also display identities that report indirectly to you, deselect the **Show only direct reports** option.

4. (Optional) To display details of an identity, click it in the list.

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. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose main data you want to display/edit.

4. In the **Edit Identity** pane, expand the one of the sections.

5. Make your changes in the corresponding fields:

   You can edit the following main data.

Table 23: 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.

Property	Description
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Resetting the password through the help desk is permitted.	Select the check box to allow password help desk staff to reset the identity's password in the Operations Support Web Portal.
Identity does not pose a security risk/Identity poses a security risk	Toggle the switch to specify whether the identity poses a security risk or not (see Marking my identities as security risks on page 166).
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 date (see Assigning other managers to my identities on page 167).
Permanently deactivated	Select the check box if you want the identity to be permanently deactivated (see Deactivating my identities on page 166).
Temporarily disabled	Select the check box if you want to deactivate the identity only temporarily.
Location information	
Primary location	Click **Assign**/**Change** and select the identity's primary location.

Property	Description
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.
Country	In the menu, select the country where the identity works.
State	In the menu, select the state where the identity works.

6. Click **Save**.

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. Open the home page.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click **Create identity**.
4. In the **Create identity** pane, enter the identity's main data in the respective fields.

   You can edit the following main data.

Table 24: Identities main data

Property	Description
Unique data	
First name	Enter the identity's first name.
Last name	Enter the identity's last name.
Central user account	Enter the name of the identity's central user account.
Default email	Enter the identity's default email address.

Property	Description
address	
Personal data	
Second 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.
Resetting the password through the help desk is permitted.	Select the check box to allow password help desk staff to reset the identity's password in the Operations Support Web Portal.
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.
Identity	Select the identity type of the identity: • **Primary identity**: Default identity for an identity. The identity has a default user account. • **Organizational identity**: Virtual identity (sub identity) for mapping different roles of an identity within the organization. The sub identity is associated with a user account of the **Organizational identity** type. In addition, specify a main identity. • **Personal administrator identity**: Virtual identity (sub identity) associated with a user account of type **Personal administrator identity** type. In addition, specify a main identity. • **Sponsored identity**: Pseudo identity associated with a user account of type **Sponsored identity**. Also assign a manager to the identity. • **Shared identity**: Pseudo identity associated with an administrative user account of type **Shared identity**. Also assign a manager to the identity.

Property	Description
	• **Service identity**: Pseudo identity associated with a user account of type **Service identity**. Also assign a manager to the identity. • **Machine identity**: Pseudo identity for mapping machine identities. For more information about mapping multiple identities of one identity, see the *One Identity Manager Identity Management Base Module Administration Guide*.
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 date (see Assigning other managers to my identities on page 167).
Permanently deactivated	Select the check box if you want the identity to be permanently deactivated (see Deactivating my identities on page 166).
Temporarily disabled	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.
Details of the location.	
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.

Property	Description
Country	In the menu, select the country where the identity works.
State	In the menu, select the state where the identity works.

5. Click **Create**.

   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.

Displaying my identities' risk indexes

You can display identities' risk indexes that you are responsible for and analyze how they are put together.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display and analyze an identity's risk index

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose risk index you want to display and analyze.

4. In the **Edit Identity** pane, click ⋮ (**Actions**) > **Analyze risk**.

Deactivating my identities

You can deactivate identities permanently such as when an employee leaves a company. This may be necessary to strip these identities of their permissions in the connected target system and from their company resources.

Effects of permanent deactivating an identity are:

- The identity cannot be assigned to identities as a manager.
- The identity cannot be assigned to roles as a supervisor.
- The identity cannot be assigned to attestation policies as an owner.
- The identity's user accounts are locked or deleted and then removed from group memberships.

To deactivate an identity

1. Open the home page.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity you want to deactivate.
4. In the **Edit Identity** pane, expand the **Organizational information** section.
5. In the **Organizational Information** section, select the **Permanently deactivated** check box.
6. Click **Save**.

Reactivating my identities

You can activate permanently deactivated identities if they have not been deactivated by certification.

To reactivate an identity

1. Open the home page.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity you want to activate.
4. In the **Edit Identity** pane, expand the **Organizational information** section.
5. In the **Organizational Information** pane, clear the **Permanently deactivated** check box.
6. Click **Save**.

Marking my identities as security risks

You can mark identities that you manage as a security risk. Then the user accounts and resources of the affected identity are blocked.

To mark an identity as a security risk

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity you want to mark as a security risk.

4. In the **Edit Identity** pane, toggle the switch next to **Identity poses a security risk**.

5. In the **Mark Identity as Security Risk** dialog, confirm the prompt with **Yes**.

   The text next to the switch changes to **Identity poses a security risk**.

6. Click **Save**.

Related topics

- Displaying and editing my identities' main data on page 160

Revoking my identities' security risks

If identities that you manage have been marked as a security risk, you can unmark them again. Then the affected identity regains access to user accounts and resources.

To revoke an identity's security risk

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the relevant identity.

4. In the **Edit Identity** pane, toggle the switch next to **Identity poses a security risk**.

5. In the **Resolve Security Risk** dialog, confirm the prompt with **Yes**.

   The text next to the switch changes to **Identity does not pose a security risk**.

6. Click **Save**.

Related topics

- Displaying and editing my identities' main data on page 160

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. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity that you want to assign to a new manager.

4. In the **Edit Identity Data** pane, click **Assign to new manager**.

5. On the **Shopping Cart** page, click **Edit** next to **Assign new manager**.

6. In the **New manager assignment** pane, in the **New manager** menu, select the manager you want to assign to the identity.

7. (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.

8. (Optional) In the **Reason** field, enter why you are assigning a new manager.

9. (Optional) In the **Priority** menu, select the priority.

10. (Optional) To specify from when the new manager is responsible for the identity, enter the date in the **Valid from** field. If you leave the field blank, the change of manager will be carried out immediately after the new manager is approved.

11. Click **Save**.

12. On the **Shopping Cart** page, click **Submit**.

    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 89). After the new manager approves this requests, the new manager is assigned.

Related topics

- Approving new managers' pending requests on page 89

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. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity for which you want to create the passcode.

4. In the **Edit Identity Data** pane, click **Create passcode**.

   The generated passcode and its validity are displayed in a dialog.

5. Note or copy the code and have it sent to the identity.

Creating reports about my identities

You can create the following reports on identities:

- Reports on individual identities
- Reports on a specific identity that reports directly to you
- Reports on all identities that report directly to you
- Reports on user accounts assigned to identities that report directly to you

To create a report on an individual identity

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity for which you want to create a report.

4. In the **Edit Identity** pane, click ⋮ (**Actions**) > **Download report**.

To create a report on identities that report to a specific identity

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity to create a report on the identities who report directly to them.

4. In the **Edit Identity** section, click ⋮ (**Actions**) > **Download report on identities who report directly to this identity**.

To create a report on all identities that report directly to you

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click ⋮ (**Actions**) > **Download report on identities who report directly to you**.

To create a report on user accounts assigned to identities that report directly to you

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click ⋮ (**Actions**) > **Download report on user accounts of my identities**.

Managing my identities' memberships

Identity assignments to company structures and entitlements are enabled through membership in the respective company structures. For example, if an identity is going to be assigned to a particular department, it must first have membership in that department.

Detailed information about this topic

Displaying my identities' departments

You can display departments that are assigned identities for which you are responsible.

To display an identity's departments

1. Open the home page.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity whose departments you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Departments**.

Displaying my identities' application roles

You can display application roles that are assigned identities for which you are responsible.

To display an identity's application roles

1. Open the home page.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity whose application roles you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **Application roles**.

Displaying my identities' user accounts

You can display user accounts that are assigned identities for which you are responsible.

To display an identity's user accounts

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose user accounts you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **User accounts**.

Displaying my identities' business roles

You can display business roles that are assigned identities for which you are responsible.

To display an identity's business roles

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose business roles you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **Business roles**.

Displaying my identities' cost centers

You can display cost centers that are assigned identities for which you are responsible.

To display an identity's cost centers

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose cost centers you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **Cost centers**.

Displaying my identities' shops

You can display shops that are assigned identities for which you are responsible.

To display an identity's shops

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose shops you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **Shops**.

Displaying my identities' locations

You can display locations that are assigned identities for which you are responsible.

To display an identity's locations

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose locations you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **Locations**.

Displaying my identities' system entitlements

You can display system entitlements that are assigned identities for which you are responsible.

To display an identity's system entitlements

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose system entitlements you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **System entitlements**.

Displaying my identities' system roles

You can display system roles that are assigned identities for which you are responsible.

To display an identity's system roles

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose system roles you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **System roles**.

Displaying identities' organizational charts

You can display the organizational charts of identities for which you are responsible.

To display an identity's organizational chart

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose organizational charts you want to display.

4. In the **Edit Identity** pane, click the **Organizational Chart** tab.

Displaying my identities' history

You can display the history of identities for which you are responsible.

To display an identity's history

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose history you want to display.

4. In the **Edit Identity** pane, click the **History** tab.

Managing my identities' attestation cases

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 my identities on page 174
- Approving and denying attestation cases of my identities on page 174

Displaying attestation cases of my identities

You can display 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. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose attestation cases you want to display.

4. In the **Edit Identity** pane, click the **Attestation** tab.

   This displays all the identity's attestation cases.

5. (Optional) To display more details of an attestation case, click **Details** next to the attestation case.

Related topics

- Attestation on page 101
- Displaying pending attestation cases on page 120

Approving and denying attestation cases of my identities

You can grant or deny approval to attestation cases of identities for which you are responsible.

To approve an attestation case

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose attestation cases are pending your approval.

4. In the **Edit Identity** pane, click the **Attestation** tab.

5. On the **Attestation** tab, click ▼ (**Filter**).

6. In the filter context menu, select the **Pending** option.

7. Perform one of the following actions:

   - To approve an attestation case, in the list, select the check box next to the attestation case and click **Approve** below the list.

   - To deny an attestation case, in the list, select the check box next to the attestation case and click **Deny** below the list.

8. (Optional) In the **Approve Attestation Case** or the **Deny Attestation Case** pane, perform the following actions:

   a. In the **Reason for your decision** field, select a standard reason for your approval decision.

   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

9. Click **Save**.

Related topics

- Attestation on page 101
- Granting or denying attestation cases on page 121

Displaying my identities' rule violations

You can display the rule violations of identities for which you are responsible.

You can also display mitigating controls for each rule violation.

To display identities' rule violations

1. Open the home page.

2. On the home page, click **Show** in the **My Direct Reports** tile.

3. On the **Identities** page, click the identity whose rule violations you want to display.

4. In the **Edit Identity** pane, click the **Rule Violations** tab.

5. (Optional) To display the mitigating controls of a rule violation, click **View mitigating controls** next to the rule violation.

Related topics

- Displaying compliance rules and rule violations on page 130

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

You can display all the cost centers for which you are responsible.

To display cost centers

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

   This opens the **Cost Centers** page and displays all the cost centers for which you are responsible.
3. (Optional) To display details of a cost center, next to the cost center, click **Edit**.

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. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.
3. On the **Cost Centers** page, next to the cost center whose main data you want to show/edit, click **Edit**.
4. In the **Edit Cost Center** pane, make your changes in the corresponding fields.

You can edit the following main data.

Table 25: 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	Select the manager who is responsible for the cost center.
2nd Manager	Select an identity to act as a deputy to the cost center's manager.
Additional manager	Click **Assign**/**Change** and select a cost center. Members of the selected application role are responsible for the department.
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.

5. Click **Save**.

Copying/splitting my cost centers

You can copy or move memberships and entitlements from cost centers you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a cost center or move memberships and entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center you want to copy or whose memberships and entitlements you want to move, click **Edit**.

4. In the **Edit Cost Center** pane, click ⁝ (**Actions**) > **Split**.

5. In the **Split** pane, In the **Type of new role** menu, select which type to give the new object.

6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

   TIP: After the object has been created, you can add the remaining main data (see Displaying and editing my department main data on page 135, Displaying and editing my business roles' main data on page 151, Displaying and editing my cost center main data on page 176, or Displaying and editing my locations' main data on page 184).

7. Click **Continue**.

8. In the **Select assignments to be copied or moved to the new role** step, perform the following actions:

   - To neither copy nor move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep this assignment**. The entitlement/membership is later only available in the source object.

   - To copy or move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new role**. The entitlement/membership is included later in the source object as well as the target object.

   - To move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new role**. The entitlement/membership is later removed from the source object and only included in the target object.

9. Click **Continue**.

10. (Optional) In the **Verify** step, you verify the actions to run and deselect the check box in front of any actions that should not be run.

11. Click **Continue**.

Related topics

- Managing my cost center memberships on page 179
- Managing my cost centers' entitlements on page 182

Managing my cost center memberships

As soon as an identity is assigned to a cost center, the identity becomes a member in the cost center.

Detailed information about this topic

- Displaying memberships in my cost centers on page 179
- Analyzing assignments to my cost centers on page 179
- Adding identities to my cost centers on page 180
- Removing identities from my cost centers on page 181

Displaying memberships in my cost centers

You can display identities that are assigned cost centers for which you are responsible.

To display identities that are assigned a cost center

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.
3. On the **Cost Centers** page, next to the cost center whose memberships you want to display, click **Edit**.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To display all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my cost centers

You can see how a cost center assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.
3. On the **Cost Centers** page, next to the cost center whose memberships you want to display, click **Edit**.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

Adding identities to my cost centers

You can assign identities to cost centers for which you are responsible.

The following assignment options are available:

- Assignment by request
- Automatic assignment through a dynamic role
- Revoking exclusion of a member

To assign an identity to a cost center using a request

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center you want to add an identity to, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Click **Request memberships**.

7. In the **Select Identities** pane, select the check box next to the identity you want to assign to the cost center.

8. Click **Request memberships**.

9. Close the **Edit Cost Center** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the cost center.

To add members automatically through a dynamic role

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

3. On the **Cost centers** page, next to the cost center for which you want to create a dynamic role, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.

6. Click **Create dynamic role**.

7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:

a. In the **Property** menu, select the relevant property.

b. In the **Operator** menu, select a logical operator.

c. In the final field, specify a comparison value.

d. (Optional) To add another condition, click **Add another condition** and repeat the steps.

e. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

TIP: To remove a condition, click 🗑 (**Delete**).

For more information about customizing filter conditions, see Custom filter conditions.

8. Click **Save**.

9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.

10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.

11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center you want to add again, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.

7. Click **Remove exclusion**.

Related topics

- Requesting products on page 61

Removing identities from my cost centers

You can remove cost centers from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a cost center from an identity

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center with a membership you want to delete, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

9. If the member was assigned through a dynamic role, perform the following actions:

   a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.

   b. Click **Exclude members**.

Managing my cost centers' 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 my cost center entitlements

You can display entitlements that are assigned cost centers for which you are responsible.

To display entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center whose entitlements you want to display, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Permissions** tab.

Adding entitlements to my cost centers

You can add entitlements to cost centers for which you are responsible. You do this through requests.

To add an entitlement to a cost center

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center you want to add an entitlement to, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, click **Request entitlements**.

6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.

7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.

9. Close the **Edit Cost Center** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    After the request has been granted approval, the entitlement is added to the cost center.

Related topics

- Requesting products on page 61

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center whose entitlement you want to delete, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.

6. Click **Remove**.

7. Confirm the prompt with **Yes** in the dialog.

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center whose rule violations you want to display, click **Edit**.

4. On the **Edit Cost Center** pane, click the **Rule Violations** tab.

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 184
- Displaying and editing my locations' main data on page 184
- Copying/splitting my locations on page 186
- Managing my location memberships on page 187
- Managing my locations' entitlements on page 190
- Displaying my locations' rule violations

Displaying my locations

You can display all the locations for which you are responsible.

To display locations

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

   This opens the **Locations** page and displays all the locations for which you are responsible.

3. (Optional) To display details of a location, next to the location, click **Edit**.

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location whose main data you want to show/edit, click **Edit**.

4. In the **Edit Location** pane, make your changes in the corresponding fields.

   You can edit the following main data.

Table 26: 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	Select the manager who is responsible for the location.
2nd Manager	Select an identity to act as a deputy to the location's manager.
Additional manager	Click **Assign**/**Change** and select a cost center. Members of the selected application role are responsible for the location.
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.
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.

5. Click **Save**.

Copying/splitting my locations

You can copy or move memberships and entitlements from locations you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a location or move memberships and entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location you want to copy or whose memberships and entitlements you want to move, click **Edit**.

4. In the **Edit Location** pane, click ⋮ (**Actions**) > **Split**.

5. In the **Split** pane, In the **Type of new role** menu, select which type to give the new object.

6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

   TIP: After the object has been created, you can add the remaining main data (see Displaying and editing my department main data on page 135, Displaying and editing my business roles' main data on page 151, Displaying and editing my cost center main data on page 176, or Displaying and editing my locations' main data on page 184).

7. Click **Continue**.

8. In the **Select assignments to be copied or moved to the new role** step, perform the following actions:

   - To neither copy nor move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep this assignment**. The entitlement/membership is later only available in the source object.

   - To copy or move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new role**. The entitlement/membership is included later in the source object as well as the target object.

   - To move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new role**. The entitlement/membership is later removed from the source object and only included in the target object.

9. Click **Continue**.

10. (Optional) In the **Verify** step, you verify the actions to run and deselect the check box in front of any actions that should not be run.

11. Click **Continue**.

Related topics

Managing my location memberships

As soon as an identity is assigned to a location, the identity becomes a member in the location.

Detailed information about this topic

Displaying memberships in my locations

You can display identities that are assigned locations for which you are responsible.

To display identities that are assigned a location

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Locations**.
3. On the **Locations** page, next to the location whose memberships you want to display, click **Edit**.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To display all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my locations

You can see how a location assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location whose memberships you want to display, click **Edit**.

4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

Adding identities to my locations

You can assign identities to locations for which you are responsible.

The following assignment options are available:

- Assignment by request
- Automatic assignment through a dynamic role
- Revoking exclusion of a member

To assign an identity to a location using a request

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location you want to add an identity to, click **Edit**.

4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Click **Request memberships**.

7. In the **Select Identities** pane, select the check box next to the identity you want to assign to the location.

8. Click **Request memberships**.

9. Close the **Edit Location** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

   Once the request has been granted approval, the identity is assigned to the location.

To add members automatically through a dynamic role

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location for which you want to create a dynamic role, click **Edit**.

4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.

6. Click **Create dynamic role**.

7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:

   a. In the **Property** menu, select the relevant property.

   b. In the **Operator** menu, select a logical operator.

   c. In the final field, specify a comparison value.

   d. (Optional) To add another condition, click **Add another condition** and repeat the steps.

   e. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

   TIP: To remove a condition, click 🗑 (**Delete**).

   For more information about customizing filter conditions, see Custom filter conditions.

8. Click **Save**.

9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.

10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.

11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location you want to add again, click **Edit**.

4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.

7. Click **Remove exclusion**.

Related topics

- Requesting products on page 61

Removing identities from my locations

You can remove locations from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

ONE IDENTITY
by Quest

To remove a location from an identity

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location with a membership you want to delete, click **Edit**.

4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

9. If the member was assigned through a dynamic role, perform the following actions:

   a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.

   b. Click **Exclude members**.

Managing my locations' 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 my locations' entitlements

You can display entitlements that are assigned locations for which you are responsible.

To display entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location whose entitlements you want to display, click **Edit**.

4. In the **Edit Locations** pane, click the **Permissions** tab.

Adding entitlements to my locations

You can add entitlements to locations for which you are responsible. You do this through requests.

To add an entitlement to a location

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location you want to add an entitlement to, click **Edit**.

4. In the **Edit Locations** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, click **Request entitlements**.

6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.

7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.

9. Close the **Edit Location** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

   After the request has been granted approval, the entitlement is added to the location.

Related topics

- Requesting products on page 61

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location whose entitlement you want to delete, click **Edit**.

4. In the **Edit Locations** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.

6. Click **Remove**.

7. Confirm the prompt with **Yes** in the dialog.

Displaying my locations' rule violations

You can see the rule violations of locations for which you are responsible.

To display rule violations

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **Locations**.

3. On the **Locations** page, next to the location whose rule violations you want to display, click **Edit**.

4. On the **Edit Location** pane, click the **Rule Violations** tab.

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 192
- Displaying and editing my system entitlements' main data on page 193
- Creating reports about my system entitlements on page 194
- Making my system entitlements requestable on page 195
- Managing my system entitlements' service items on page 196
- Managing my system entitlement memberships on page 199
- Managing my system entitlements' child groups on page 202
- Managing my system entitlements' attestation cases on page 202

Displaying my system entitlements

You can display all the system entitlements for which you are responsible.

To display system entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

   This opens the **System Entitlements** page and displays all the system entitlements for which you are responsible.

3. (Optional) To display only system entitlements that are assigned to a specific target system, perform the following actions:

   a. Click ⛁ (**target system**).

   b. In the **Narrow the selection further down by: Target system** dialog box, select the check box next to the target system whose system entitlements you want to display.

      > TIP: To display target systems that are under a target system, click ▸ (**expand**).

   c. Click **Apply**.

4. (Optional) To display details of a system entitlement, click it in the list.

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlements whose main data you want to display/edit.

4. In the **Edit System Entitlement** pane, make your changes in the corresponding fields.

You can edit the following main data.

Table 27: 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.
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.
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.

5. Click **Save**.

Creating reports about my system entitlements

You can create reports about system entitlement data.

To create a report about a system entitlement

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement for which you want to create a report.

4. In the **Edit Entitlement** pane, click ⋮ (**Actions**) > **Download report**.

Making my system entitlements requestable

To be able to request a system entitlements in the Web Portal, the system entitlement must fulfill the following prerequisites:

- The system entitlement must be assigned to a service item (see Managing my system entitlements' service items on page 196).

- The system entitlement must be assigned to a shelf in a shop (see Adding products to shelves on page 48).

- The system entitlement must be marked as requestable (see following step-by-step).

To make a system entitlement requestable

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. (Optional) To display only those system entitlements only that are not marked as requestable, perform the following actions:

    a. Click ▼ (**Filter**).

    b. In the filter context menu, select the **Not requestable** check box.

4. In the list, select the check box in front of the system entitlement that you want to make requestable.

5. Under the list, set the switch to **Make selected items requestable** and click **Update**.

    TIP: If you do not want the system entitlement to be requested in the Web Portal anymore, set the switch to **Make selected items not requestable**.

Related topics

- Managing shops on page 39
- Managing my system entitlements' service items on page 196
- Adding products to shelves on page 48

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. Open the home page.

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**.

Managing my system entitlements' service items

To be able to request system entitlements as products, they are assigned to corresponding service items. Then you can assign these service items to a shop (see Managing requestable products in shops on page 48).

Detailed information about this topic

- Specifying my system entitlement owners on page 195
- Editing my system entitlements' service items on page 196

Editing my system entitlements' service items

You can edit the main data of service items.

To display and edit a service items role's main data

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose service item you want to edit.

4. In the **Edit System Entitlement** pane, click the **Service Item** tab.

5. On the **Service Item** tab, edit the service item's main data.

Table 28: Main data of system entitlement service items

Property	Description
Service item	Enter a name for the service item.
Description	Enter a description of the service item.
Service category	You can group different service items into service categories. To do this, click **Assign**/**Change** and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 49.
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Approval by multi-factor authentication	Select this check box to specify that approvals of requests for this service item require multi-factor authentication.
Max. days valid	Specify how long an identity can keep the product until it is automatically unsubscribed again. An identity keeps their requested products on the shelf until they unsubscribe from them themselves. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. Products that are intended to have a limited shelf life need to be marked with a validity period.
Website	Specify the URL of a web page that contains more information about the product. Use the following format: **https://www.example.com** or **http://www.example.com**. This field allows you to link product descriptions in the internet or intranet to the service item.
Sort order	Specify how the service category is sorted.
Request property	Select the request property using the additional request parameters that are defined for a request. If you do not select any request properties, the request properties of the associated service category are used.

Property	Description
	Requests can be given additional information though product-specific request properties such as the specific details of a product, its size, or color. A request property gathers all additional features together that can be given when requesting a product.
Functional area	Click **Assign**/**Change** and then select the functional area to which you want to assign the service item. You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by functional area. To do this, service items must be assigned to functional areas. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Attestors	Click **Assign**/**Change** and then select an application role. Members of this application role can approve attestation cases that affect the service item.
Terms of use	Select the terms of use that the product's requester must accept.
Picture	Enter a picture for the service item. Users see this picture when they make a request. Perform the following actions as well: 1. Click **Add**/**Change**. 2. Select an image from your medium.
Request parameters must be defined per recipient	Select the check box to enter additional request properties separately for each recipient of this product, if the product is requested for different recipients in one request procedure.
Retain service item assignment on relocation	Select the check box if requests for this service item are retained when a customer or the product is moved. If an identity requests a product from a Shop and changes the Shop at a later date, a decision must be made about how to proceed with the existing request. The same applies if a product is moved to another shelf.
Tags	Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.
Not	Set the switch to **Requestable** if you want to request

Property	Description
requestable/Requestable	system entitlements through the Web Portal.
	Set the switch to **Not requestable** if you do not want to request system entitlements through the Web Portal.
	For more information, see Making system entitlements requestable on page 232.
Product owner	Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item.
	Specify which identities are responsible for the service item.
	• 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**.

Related topics

- Assigning owners to system entitlements on page 213

Managing my system entitlement memberships

As soon as a system entitlement has been assigned to an identity using a corresponding user account, the identity becomes a member in the system entitlement.

Detailed information about this topic

- Displaying memberships in my system entitlements on page 200
- Analyzing assignments to my system entitlements on page 200
- Assigning identities to my system entitlements on page 201
- Removing identities from my system entitlements on page 201

Displaying memberships in my system entitlements

You can display identities that are assigned system entitlements for which you are responsible.

To display identities that are assigned a system entitlement

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose memberships you want to display.

4. In the **Edit System Entitlement** pane, click the **Memberships** tab.

5. (Optional) To display all memberships that were created directly in the selected system entitlement, click **Direct memberships**.

6. (Optional) To display all memberships created by inheritance from child system entitlements, click **Inherited memberships**.

Analyzing assignments to my system entitlements

You can see how a system entitlement assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose memberships you want to display.

4. In the **Edit System Entitlement** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Direct memberships** or **Inherited memberships**.

6. Next to the appropriate membership, click **View assignment analysis**.

Assigning identities to my system entitlements

You can assign identities to system entitlements for which you are responsible. You do this with a request.

To assign an identity to a system entitlement using a request

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement to which you want to assign an identity.

4. In the **Edit System Entitlement** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Request memberships**.

6. In the **Select Identities** pane, select the check box next to the identity you want to assign to the system entitlement.

7. Click **Apply**.

8. Close the **Edit System Entitlement** pane.

9. In the menu bar, click **Requests** > **Shopping cart**.

10. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the system entitlement.

Related topics

- Requesting products on page 61

Removing identities from my system entitlements

You can remove system entitlements from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a system entitlement from an identity

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement with a membership you want to delete.

4. In the **Edit System Entitlement** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Direct Memberships**.

6. Select the check box next to the membership you want to delete.

7. Perform one of the following actions:

- If it is a direct assignment, click **Delete**.

- If it is an indirect assignment, click **Unsubscribe**.

  NOTE: You can only unsubscribe memberships that you have requested yourself.

8. In the **Delete Memberships** or **Unsubscribe Memberships** dialog, confirm the prompt with **OK**.

Managing my 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

- Display my system entitlements' child groups on page 202

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose child groups you want to display.

4. In the **Edit System Entitlement** pane, click the **Child System Entitlements** tab.

Managing my system entitlements' attestation cases

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 203
- Approving and denying my system entitlements' attestation cases on page 203

Displaying my system entitlements' attestation cases

You can display 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. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. In the **Edit System Entitlement** pane, click the **Attestation** tab.

   This displays all the system entitlement's attestation cases.
5. (Optional) To display more details of an attestation case, click **Details** next to the attestation case.

Related topics

- Attestation on page 101
- Displaying pending attestation cases on page 120

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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose attestation cases are pending your approval.

4. In the **Edit System Entitlement** pane, click the **Attestation** tab.

5. On the **Attestation** tab, click ▼ (**Filter**).

6. In the filter context menu, select the **Pending** option.

7. Perform one of the following actions:

   - To approve an attestation case, in the list, select the check box next to the attestation case and click **Approve** below the list.

   - To deny an attestation case, in the list, select the check box next to the attestation case and click **Deny** below the list.

8. (Optional) In the **Approve Attestation Case** or the **Deny Attestation Case** pane, perform the following actions:

   a. In the **Reason for your decision** field, select a standard reason for your approval decision.

   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

9. Click **Save**.

Related topics

- Attestation on page 101
- Granting or denying attestation cases on page 121

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' rule violations

Displaying my system roles

You can display all the system roles for which you are responsible.

To display system roles

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System roles**.

   This opens the **System Roles** page and displays all the system roles for which you are responsible.
3. (Optional) To display details of a system role, click **Edit** next to the system role.

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. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System roles**.
3. On the **System Roles** page, next to the system role whose main data you want to show/edit, click **Edit**.
4. In the **Edit System Role** pane, make your changes in the corresponding fields.

You can edit the following main data.

Table 29: 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	Shows you the associated service item.
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.

5. Click **Save**.

Managing my system role memberships

As soon as a system role is assigned to an identity, the identity becomes a member in the system role.

Detailed information about this topic

Displaying memberships in my system roles

You can display identities that are assigned system roles for which you are responsible.

To display identities that are assigned a system role

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System roles**.
3. On the **System Roles** page, next to the system role whose memberships you want to display, click **Edit**.
4. In the **Edit System Role** pane, click the **Memberships** tab.

Analyzing assignments to my system roles

You can see how a system role assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System roles**.
3. On the **System Roles** page, next to the system role whose memberships you want to display, click **Edit**.
4. In the **Edit System Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, select the check box next to the corresponding membership.
6. Click **View assignment analysis**.

Assigning identities to my system roles

You can assign identities to system roles for which you are responsible. You do this with a request.

To assign an identity to a system role using a request

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System roles**.

3. On the **System Roles** page, next to the system role you want to add an identity to, click **Edit**.

4. In the **Edit System Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Request memberships**.

6. In the **Select Identities** pane, select the check box next to the identity you want to assign to the system role.

7. Click **Request memberships**.

8. Close the **Edit System Role** pane.

9. In the menu bar, click **Requests** > **Shopping cart**.

10. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the system role.

Related topics

- Requesting products on page 61

Removing identities from my system roles

You can remove system roles from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a system role from an identity

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System roles**.

3. On the **System Roles** page, next to the system role with a membership you want to delete, click **Edit**.

4. In the **Edit System Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

Managing 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

You can display entitlements that are assigned system roles for which you are responsible.

To display entitlements

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System roles**.

3. On the **System Roles** page, next to the system role whose entitlements you want to display, click **Edit**.

4. In the **Edit System Role** pane, click the **Permissions** tab.

Adding entitlements to my system roles

You can add entitlements to system roles for which you are responsible. You do this through requests.

To add an entitlement to a system role

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click **System roles**.

3. On the **System Roles** page, next to the system role you want to add an entitlement to, click **Edit**.

4. In the **Edit System Role** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, click **Request entitlements**.

6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.

7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.

9. Close the **Edit System Role** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    After the request has been granted approval, the entitlement is added to the system role.

Related topics

- Requesting products on page 61

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. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System roles**.
3. On the **System Roles** page, next to the system role whose entitlement you want to delete, click **Edit**.
4. In the **Edit System Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

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. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System roles**.
3. On the **System Roles** page, next to the system role whose rule violations you want to display, click **Edit**.
4. On the **Edit System Role** pane, click the **Rule Violations** tab.

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

You can see delegations created by you or by others for you.

To display delegations

1. In the menu bar, click **Requests** > **Request History**.

2. On the **Request History** page, click ▼ (**Filter**).

3. In the filter context menu, select the **My delegations** check box.

4. (Optional) To see more details of a delegation, click **Details** next to the corresponding delegation.

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 212) and create a new delegation.

To create a delegation

1. In the menu bar, click **Responsibilities** > **Delegation**.

2. On the **Create Delegation** page, in the **Delegation recipient** field, select the identity to which you want to delegate.

3. Click **Next**.

4. In the **Select the type of delegation** step, perform one of the following actions:
   - To delegate all memberships and responsibilities (grouped by topic), set **Delegate all memberships and responsibilities**.
   - To delegate individual memberships and responsibilities, set **Select individual memberships and responsibilities to delegate**.

5. Click **Next**.

6. In the **Select the role membership/responsibility you want to delegate** 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**.

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 212).

To cancel a delegation

1. In the menu bar, click **Requests** > **Request History**.

2. On the **Request History** page, click ▼ (**Filter**).

3. In the filter context menu, select the **My delegations** check box.

4. Next to the delegation you want to cancel, click **Details**.

5. In the **View Request Details** pane, click **Cancel request**.

6. (Optional) In the **Cancel request** pane, in the **Reason for your decision** field, enter a reason for the cancellation.

7. Click **Save**.

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 212).

To delete a delegation

1. In the menu bar, click **Requests** > **Request History**.

2. On the **Request History** page, click ▼ (**Filter**).

3. In the filter context menu, select the **My delegations** check box.

4. Next to the delegation you want to delete, click **Details**.

5. In the **View Request Details** pane, click **Unsubscribe product**.

6. In the **Unsubscribe Product** pane, perform the following actions:

   a. In the **Unsubscribed as from** field, specify the date on which to delete the delegation. If you leave this field empty, the delegation is deleted once you have clicked **Saved**.

   b. In the **Reason for your decision** field, enter a reason for your approval decision.

   c. In the **Additional comments about your decision** field, enter extra information.

   d. Click **Save**.

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 213
- Assigning owners to devices on page 214

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. You can also take responsibility for system entitlement yourself.

To assign system entitlements to an owner

1. In the menu bar, click **Responsibilities** > **System entitlement ownership**.

2. On the **Assign an Owner for a System Entitlement** page, in the **System entitlement** menu, select the system entitlement that you want to assign a owner to.

3. Click **Next**.

4. In the second step, perform one of the following actions:

   - To take responsibility yourself, click **I want to take ownership of this system entitlement**.

   - To specify another identity as the owner, click **Select another owner** or **Select from the suggested possible owners** and select the respective identity in the **Designated owner** menu.

5. Click **Next**.

   In the context of an attestation, the selected owner can confirm that this assignment is correct (see Pending attestations on page 120).

Related topics

- Assigning owners to devices on page 214

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. You can also take responsibility for the device yourself.

To assign an owner to a device

1. In the menu bar, click **Responsibilities** > **Device ownership**.

2. On the **Assign an Owner for a Device** page, in the **Device** field, click **Assign**.

3. In the **Device** pane, click the device that you want to assign an owner to.

4. Click **Next**.

5. In the second step, perform one of the following actions:

   - To take responsibility yourself, click **I want to take ownership of this device**.

   - To specify another identity as the owner, click **Select another owner** or **Select from the suggested possible owners** and select the respective identity in the **Designated owner** menu.

6. Click **Next**.

   In the context of an attestation, the selected owner can confirm that this assignment is correct (see Pending attestations on page 120).

Related topics

- Assigning owners to system entitlements on page 213

Managing data

The Web Portal provides you with comprehensive functionality for managing the following objects.

- Identities
- User accounts
- System entitlements
- Departments
- Locations
- Cost centers
- Business roles
- System roles

Detailed information about this topic

Managing identities

You can use the Web Portal to manage identities.

Detailed information about this topic

Displaying identities

You can display any of the identities and their details.

To display identities

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation click **Identities**.

   This opens the **Identities** page and displays all the identities.
3. (Optional) To display details of an identity, click it in the list.

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 **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click **Create identity**.

   You can edit the following main data.

Table 30: Identities main data

Property	Description
Unique data	
First name	Enter the identity's first name.
Last name	Enter the identity's last name.
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Personal data	
Second 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.
Resetting the password through the help desk is permitted.	Select the check box to allow password help desk staff to reset the identity's password in the Operations Support Web Portal.
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.
Identity	Select the identity type of the identity: • **Primary identity**: Default identity for an identity. The identity has a default user account. • **Organizational identity**: Virtual identity (sub identity) for mapping different roles of an identity within the

Property	Description
	organization. The sub identity is associated with a user account of the **Organizational identity** type.
	In addition, specify a main identity.
	• **Personal administrator identity**: Virtual identity (sub identity) associated with a user account of type **Personal administrator identity** type.
	In addition, specify a main identity.
	• **Sponsored identity**: Pseudo identity associated with a user account of type **Sponsored identity**.
	Also assign a manager to the identity.
	• **Shared identity**: Pseudo identity associated with an administrative user account of type **Shared identity**.
	Also assign a manager to the identity.
	• **Service identity**: Pseudo identity associated with a user account of type **Service identity**.
	Also assign a manager to the identity.
	• **Machine identity**: Pseudo identity for mapping machine identities.
	For more information about mapping multiple identities of one identity, see the *One Identity Manager Identity Management Base Module Administration Guide*.
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 date (see Assigning other managers to my identities on page 167).
Permanently deactivated	Select the check box if you want the identity to be permanently deactivated (see Deactivating my identities on page 166).
Temporarily	Select the check box to activate the identity at a later date

ONE IDENTITY
by Quest

Property	Description
disabled	then click the ▤ (**Calendar**) and use the date picker to select the date to activate the identity.
Details of the location.	
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.
Country	In the menu, select the country where the identity works.
State	In the menu, select the state where the identity works.

4. Click **Create**.

   When saving, the system checks whether the combination of first and last name already exists.

5. 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.

Displaying and analyzing identities' risk indexes

You can display identities' risk indexes and analyze how they are put together.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display and analyze an identity's risk index

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose risk index you want to display and analyze.

4. In the **Edit Identity** pane, click ⋮ (**Actions**) > **Analyze risk**.

Deactivating identities

You can deactivate identities permanently such as when an employee leaves a company. This may be necessary to strip these identities of their permissions in the connected target system and from their company resources.

Effects of permanent deactivating an identity are:

- The identity cannot be assigned to identities as a manager.

- The identity cannot be assigned to roles as a supervisor.

- The identity cannot be assigned to attestation policies as an owner.

- The identity's user accounts are locked or deleted and then removed from group memberships.

To deactivate an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity you want to deactivate.

4. In the **Edit Identity** pane, toggle the switch next to **Identity is active**.

   The text next to the switch changes to **Identity is inactive**.

5. Click **Save**.

Reactivating identities

You can activate permanently deactivated identities if they have not been deactivated by certification.

To reactivate an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity you want to activate.

4. In the **Edit Identity** pane, toggle the switch next to **Identity is inactive**.

   The text next to the switch changes to **Identity is active**.

5. Click **Save**.

Marking identities as security risks

You can mark identities as a security risk. Then the user accounts and resources of the affected identity are blocked.

To mark an identity as a security risk

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity you want to mark as a security risk.

4. In the **Edit Identity** pane, toggle the switch next to **Identity poses a security risk**.

5. In the **Mark Identity as Security Risk** dialog, confirm the prompt with **Yes**.

   The text next to the switch changes to **Identity poses a security risk**.

6. Click **Save**.

Revoking identities' security risks

If identities have been marked as a security risk, you can unmark them again. Then the affected identity regains access to user accounts and resources.

To revoke an identity's security risk

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the relevant identity.

4. In the **Edit Identity** pane, toggle the switch next to **Identity poses a security risk**.

5. In the **Resolve Security Risk** dialog, confirm the prompt with **Yes**.

   The text next to the switch changes to **Identity does not pose a security risk**.

6. Click **Save**.

Deleting identities

When an identity is deleted, they are tested to see if user accounts and company resources are still assigned, or if there are still pending requests. The identity is marked for deletion and therefore locked out of further processing. Before an identity is permanently deleted from the database, you must remove all company resource assignments and finalize all requests. If no more company resources are assigned, the identity is deleted permanently.

To delete an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity you want to delete.

4. In the **Edit Identity Data** area, click **Delete**.

5. In the **Delete Identity** dialog, confirm the prompt with **Yes**.

Assigning other managers to identities

You can assign managers to identities or remove the currently assigned manager.

To assign a manager to an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity that you want to assign to a new manager.

4. In the **Edit Identity** pane, click in the **Manager** field to select the manager you want to assign to the identity.

   TIP: To remove the current manager, in the **Manager** menu, click ✕ (**Remove assignment**).

5. Click **Save**.

Creating reports about identities

You can create the following reports on identities:

- Reports on individual identities
- Reports on a specific identity that reports directly to you
- Reports on all identities that report directly to you
- Reports on user accounts assigned to identities that report directly to you

To create a report on an individual identity

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity that you want to create a report on.
4. In the **Edit Identity**, click ⋮ (**Actions**) > **Download report**.

To create a report on identities that report to a specific identity

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity to create a report on the identities who report directly to them.
4. In the **Edit Identity** section, click ⋮ (**Actions**) > **Download report on identities who report directly to this identity**.

To create a report on all identities that report directly to you

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click ⋮ (**Actions**) > **Download report on identities who report directly to you**.

To create a report on user accounts assigned to identities that report directly to you

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click ⋮ (**Actions**) > **Download report on user accounts of my identities**.

Managing identities' memberships

Identity assignments to company structures and entitlements are enabled through membership in the respective company structures. For example, if an identity is going to be assigned to a particular department, it must first have membership in that department.

Detailed information about this topic

- Displaying identities' departments
- Displaying identities' application roles
- Displaying identities' user accounts
- Displaying identities' business roles
- Displaying identities' cost centers
- Displaying identities' shops
- Displaying identities' locations
- Displaying identities' system entitlements
- Displaying identities' system roles

Displaying identities' departments

You can display departments that are assigned identities.

To display an identity's departments

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose departments you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Departments**.

Displaying identities' application roles

You can display application roles assigned to identities.

To display an identity's application roles

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose application roles you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **Application roles**.

Displaying identities' user accounts

You can display user accounts assigned to identities.

To display an identity's user accounts

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose user accounts you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **User accounts**.

Displaying identities' business roles

You can display business roles that are assigned identities.

To display an identity's business roles

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose business roles you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **Business roles**.

Displaying identities' cost centers

You can display cost centers that are assigned identities.

To display an identity's cost centers

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose cost centers you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **Cost centers**.

Displaying identities' shops

You can display shops that are assigned identities.

To display an identity's shops

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose shops you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Shops**.

Displaying identities' locations

You can display locations that are assigned identities.

To display an identity's locations

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose locations you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Locations**.

Displaying identities' system entitlements

You can display system entitlements assigned to identities.

To display an identity's system entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose system entitlements you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **System entitlements**.

Displaying identities' system roles

You can display system roles that are assigned identities.

To display an identity's system roles

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose system roles you want to display.

4. In the **Edit Identity** pane, click the **Memberships** tab.

5. In the navigation on the **Memberships** tab, click **System roles**.

Displaying identities' organizational charts

You can display identities' organizational charts.

To display an identity's organizational chart

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose organizational charts you want to display.

4. In the **Edit Identity** pane, click the **Organizational Chart** tab.

Displaying identities' history

You can see identities' history.

To display an identity's history

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose history you want to display.

4. In the **Edit Identity** pane, click the **History** tab.

Managing attestation cases of identities

You can use the Web Portal to display all the attestation cases for identities and make approval decisions about them.

Detailed information about this topic

- Displaying attestation cases of identities on page 228
- Approving and denying attestation cases of identities on page 228

Displaying attestation cases of identities

You can see all the identities' attestation cases. In addition, you can obtain more information about the attestation cases.

To display attestation cases of an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose attestation cases you want to display.

4. In the **Edit Identity** pane, click the **Attestation** tab.

    This displays all the identity's attestation cases.

5. (Optional) To display more details of an attestation case, click **Details** next to the attestation case.

Related topics

- Attestation on page 101
- Displaying pending attestation cases on page 120

Approving and denying attestation cases of identities

You can grant or deny approval to attestation cases of identities.

To approve an attestation case

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **Identities** page, click the identity whose attestation cases you want decide.

4. In the **Edit Identity** pane, click the **Attestation** tab.

5. On the **Attestation** tab, click ▼ (**Filter**).

6. In the filter context menu, under **State**, select the **Pending** option.

7. Perform one of the following actions:

    - To approve an attestation case, in the list, select the check box next to the attestation case and click **Approve** below the list.

    - To deny an attestation case, in the list, select the check box next to the attestation case and click **Deny** below the list.

8. (Optional) In the **Approve Attestation Case** or the **Deny Attestation Case** pane, perform the following actions:

   a. In the **Reason for your decision** field, select a standard reason for your approval decision.

   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

9. Click **Save**.

Related topics

- Attestation on page 101
- Granting or denying attestation cases on page 121

Displaying identities' rule violations

You can display the rule violations of identities.

You can also display mitigating controls for each rule violation.

To display identities' rule violations

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose rule violations you want to display.
4. In the **Edit Identity** pane, click the **Rule Violations** tab.
5. (Optional) To display the mitigating controls of a rule violation, click **View mitigating controls** next to the rule violation.

Related topics

- Displaying compliance rules and rule violations on page 130

Managing user accounts

You can use the Web Portal to manage user accounts.

User accounts represent a target system's authentication objects. A user account obtains the required permissions for accessing target system resources through its memberships in groups and system entitlements.

A user account can be linked to an identity in One Identity Manager. However, you can also manage user accounts separately from identities.

Detailed information about this topic

- Displaying user accounts on page 230
- Displaying user account memberships on page 230

Displaying user accounts

You can see any of the user accounts and their details.

To display user accounts

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation click **User accounts**.

   This opens the **User accounts** page and displays all the user accounts.

3. (Optional) To display only use account that are assigned to a specific target system, perform the following actions:

   a. Click ⚓ (**target system**).

   b. In the **Narrow the selection further down by: Target system** dialog box, select the check box next to the target system whose user accounts you want to display.

   > TIP: To display target systems that are under a target system, click ▶ (**expand**).

   c. Click **Apply**.

4. (Optional) To display details of a user account, click it in the list.

Managing user account memberships

As soon as a system entitlement is assigned to a user account, the user account becomes a member in the system entitlement.

Detailed information about this topic

- Displaying user account memberships on page 230

Displaying user account memberships

You can display which system entitlements are assigned to certain user accounts.

To display memberships

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **User accounts**.

3. In the list, click the user account whose memberships you want to display.

4. In the **Edit User Account** pane, click the **Memberships** tab.

   TIP: If you click a system entitlement in the list, you will see more information and options (see Managing system entitlements on page 231).

Creating reports about user accounts

You can create reports on user account data.

To create a report on a user account

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **User Accounts** page, click the user account that you want to create a report on.

4. In the **Edit User Account**, click ⋮ (**Actions**) > **Download report**.

Managing system entitlements

You can use the Web Portal to manage 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.

Detailed information about this topic

- Displaying system entitlements on page 232
- Making system entitlements requestable on page 232
- Displaying and editing system entitlements main data on page 233
- Specifying system entitlement owners on page 234
- Managing service items for system entitlements on page 236
- Managing system entitlement memberships on page 242
- Managing system entitlement child groups on page 244
- Managing attestation cases of system entitlements on page 245
- Creating reports about system entitlements on page 247

Displaying system entitlements

You can see any of the system entitlements and their details.

To display system entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation click **System entitlements**.

   This opens the **System Entitlements** page and displays all the system entitlements.

3. (Optional) To display only system entitlements that are assigned to a specific target system, perform the following actions:

   a. Click ⛓ (**target system**).

   b. In the **Narrow the selection further down by: Target system** dialog box, select the check box next to the target system whose system entitlements you want to display.

      TIP: To display target systems that are under a target system, click ▶ (**expand**).

   c. Click **Apply**.

4. (Optional) To display details of a system entitlement, click it in the list.

Making system entitlements requestable

To be able to request a system entitlements in the Web Portal, the system entitlement must fulfill the following prerequisites:

- The system entitlement must be assigned to a service item (see Managing service items for system entitlements on page 236).

- The system entitlement must be assigned to a shelf in a shop (see Adding products to shelves on page 48).

- The system entitlement must be marked as requestable (see following step-by-step).

To make a system entitlement requestable

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System entitlements**.

3. (Optional) To display only those system entitlements only that are not marked as requestable, perform the following actions:

   a. Click ▼ (**Filter**).

   b. In the filter context menu, select the **Not requestable** check box.

4. In the list, select the check box in front of the system entitlement that you want to make requestable.

5. Under the list, set the switch to **Make selected items requestable** and click **Update**.

> TIP: If you do not want the system entitlement to be requested in the Web Portal anymore, set the switch to **Make selected items not requestable**.

Related topics

- Managing shops on page 39
- Managing service items for system entitlements on page 236
- Adding products to shelves on page 48

Displaying and editing system entitlements main data

You can see and edit system entitlements' main data.

To display and edit a system entitlement's main data

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose main data you want to display.

4. In the **Edit System Entitlement** pane, make your changes in the relevant fields.

Table 31: 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.
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.
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.

5. Click **Save**.

Specifying system entitlement owners

You can specify which identities are responsible for 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. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, 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**.

To specify owners for several system entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System entitlements**.

3. On the **System Entitlements** page, select the check box in front of the system entitlements whose owners you want to specify.

4. Click **Assign product owner**.

5. In the **Assign Product Owner** pane, perform 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 **Apply**.

Managing service items for system entitlements

To be able to request system entitlements as products, they are assigned to corresponding service items. Then you can assign these service items to a shop (see Managing requestable products in shops on page 48).

Detailed information about this topic

- Creating service items for system entitlements on page 236
- Specifying system entitlement owners on page 234
- Editing system entitlement service items on page 239

Creating service items for system entitlements

You can create service items for system entitlements.

To create a service item for a system entitlement

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement for which you want to create a service item.
4. In the **Edit System Entitlements** area, click the **Details** tab.
5. On the **Details** tab, click **Create service item**.
6. Click **Service Item** tab.
7. On the **Service Item** tab, edit the service item's main data.

Table 32: Main data of system entitlement service items

Property	Description
Service item	Enter a name for the service item.
Description	Enter a description of the service item.
Service category	You can group different service items into service categories. To do this, click **Assign**/**Change** and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 49.

Property	Description
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Approval by multi-factor authentication	Select this check box to specify that approvals of requests for this service item require multi-factor authentication.
Max. days valid	Specify how long an identity can keep the product until it is automatically unsubscribed again. An identity keeps their requested products on the shelf until they unsubscribe from them themselves. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. Products that are intended to have a limited shelf life need to be marked with a validity period.
Website	Specify the URL of a web page that contains more information about the product. Use the following format: **https://www.example.com** or **http://www.example.com**. This field allows you to link product descriptions in the internet or intranet to the service item.
Sort order	Specify how the service category is sorted.
Request property	Select the request property using the additional request parameters that are defined for a request. If you do not select any request properties, the request properties of the associated service category are used. Requests can be given additional information though product-specific request properties such as the specific details of a product, its size, or color. A request property gathers all additional features together that can be given when requesting a product.
Functional area	Click **Assign**/**Change** and then select the functional area to which you want to assign the service item. You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by functional area. To do this, service items must be assigned to functional areas. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.

Property	Description
Attestors	Click **Assign**/**Change** and then select an application role. Members of this application role can approve attestation cases that affect the service item.
Terms of use	Select the terms of use that the product's requester must accept.
Picture	Enter a picture for the service item. Users see this picture when they make a request. Perform the following actions as well: 1. Click **Add**/**Change**. 2. Select an image from your medium.
Request parameters must be defined per recipient	Select the check box to enter additional request properties separately for each recipient of this product, if the product is requested for different recipients in one request procedure.
Retain service item assignment on relocation	Select the check box if requests for this service item are retained when a customer or the product is moved. If an identity requests a product from a Shop and changes the Shop at a later date, a decision must be made about how to proceed with the existing request. The same applies if a product is moved to another shelf.
Tags	Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.
Not requestable/Requestable	Set the switch to **Requestable** if you want to request system entitlements through the Web Portal. Set the switch to **Not requestable** if you do not want to request system entitlements through the Web Portal. For more information, see Making system entitlements requestable on page 232.
Product owner	Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item. Specify which identities are responsible for the service item. • To specify members of a specific application role

Property	Description
	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.

8. Click **Save**.

Editing system entitlement service items

You can edit the main data of service items.

To display and edit a service items role's main data

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose service item you want to edit.
4. In the **Edit System Entitlement** pane, click the **Service Item** tab.
5. On the **Service Item** tab, edit the service item's main data.

Table 33: Main data of system entitlement service items

Property	Description
Service item	Enter a name for the service item.
Description	Enter a description of the service item.
Service category	You can group different service items into service categories. To do this, click **Assign**/**Change** and select the service category to which you want to

Property	Description
	assign the service item. For more information about service categories, see Managing service categories on page 49.
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Approval by multi-factor authentication	Select this check box to specify that approvals of requests for this service item require multi-factor authentication.
Max. days valid	Specify how long an identity can keep the product until it is automatically unsubscribed again. An identity keeps their requested products on the shelf until they unsubscribe from them themselves. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. Products that are intended to have a limited shelf life need to be marked with a validity period.
Website	Specify the URL of a web page that contains more information about the product. Use the following format: **https://www.example.com** or **http://www.example.com**. This field allows you to link product descriptions in the internet or intranet to the service item.
Sort order	Specify how the service category is sorted.
Request property	Select the request property using the additional request parameters that are defined for a request. If you do not select any request properties, the request properties of the associated service category are used. Requests can be given additional information though product-specific request properties such as the specific details of a product, its size, or color. A request property gathers all additional features together that can be given when requesting a product.
Functional area	Click **Assign**/**Change** and then select the functional area to which you want to assign the service item. You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by functional area. To do this, service items

Property	Description
	must be assigned to functional areas. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Attestors	Click **Assign**/**Change** and then select an application role. Members of this application role can approve attestation cases that affect the service item.
Terms of use	Select the terms of use that the product's requester must accept.
Picture	Enter a picture for the service item. Users see this picture when they make a request. Perform the following actions as well: 1. Click **Add**/**Change**. 2. Select an image from your medium.
Request parameters must be defined per recipient	Select the check box to enter additional request properties separately for each recipient of this product, if the product is requested for different recipients in one request procedure.
Retain service item assignment on relocation	Select the check box if requests for this service item are retained when a customer or the product is moved. If an identity requests a product from a Shop and changes the Shop at a later date, a decision must be made about how to proceed with the existing request. The same applies if a product is moved to another shelf.
Tags	Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.
Not requestable/Requestable	Set the switch to **Requestable** if you want to request system entitlements through the Web Portal. Set the switch to **Not requestable** if you do not want to request system entitlements through the Web Portal. For more information, see Making system entitlements requestable on page 232.
Product owner	Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item.

Property	Description
	Specify which identities are responsible for the service item.

- 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**.

Related topics

- Assigning owners to system entitlements on page 213

Managing system entitlement memberships

As soon as a system entitlement has been assigned to an identity using a corresponding user account, the identity becomes a member in the system entitlement.

Detailed information about this topic

- Displaying system entitlement memberships on page 242
- Analyzing assignments to system entitlements on page 243
- Assigning identity system entitlements on page 243
- Removing system entitlements from identities on page 244

Displaying system entitlement memberships

You can display which identities are assigned to certain system entitlements.

To display memberships

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System entitlements**.

3. In the list, click the system entitlement whose memberships you want to display.

4. In the **Edit System Entitlement** pane, click the **Memberships** tab.

5. (Optional) To display all memberships exist directly in the selected system entitlement, click **Direct memberships**.

6. (Optional) To display all memberships created by inheritance from child system entitlements, click **Inherited memberships**.

Analyzing assignments to system entitlements

You can see how a system entitlement assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose memberships you want to display.

4. In the **Edit System Entitlement** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Direct memberships** or **Inherited memberships**.

6. Next to the appropriate membership, click **View assignment analysis**.

Assigning identity system entitlements

You can assign system entitlements to identities. You do this through requests.

To assign an identity to a system entitlement using a request

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement to which you want to assign an identity.

4. In the **Edit System Entitlement** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Request memberships**.

6. In the **Select Identities** pane, select the check box next to the identity you want to assign to the system entitlement.

7. Click **Apply**.

8. Close the **Edit System Entitlement** pane.

9. In the menu bar, click **Requests** > **Shopping cart**.

10. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the system entitlement.

Related topics

- Requesting products on page 61

Removing system entitlements from identities

You can remove system entitlements from identities by deleting or unsubscribing the relevant memberships.

To remove a system entitlement from an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement with a membership you want to delete.

4. In the **Edit System Entitlement** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Direct Memberships**.

6. Select the check box next to the membership you want to delete.

7. Perform one of the following actions:

   - If it is a direct assignment, click **Delete**.

   - If it is an indirect assignment, click **Unsubscribe**.

     NOTE: You can only unsubscribe memberships that you have requested yourself.

8. In the **Delete Memberships** or **Unsubscribe Memberships** dialog, confirm the prompt with **OK**.

Managing system entitlement 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

You can see child groups of system entitlements.

To display the child groups of a system entitlement

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose child groups you want to display.
4. In the **Edit System Entitlement** pane, click the **Child System Entitlements** tab.

Managing attestation cases of system entitlements

You can use the Web Portal to display all the attestation cases for system entitlements and make approval decisions about them.

Detailed information about this topic

-
-

Displaying attestation cases of system entitlements

You can see all the system entitlements' attestation cases. In addition, you can obtain more information about the attestation cases.

To display attestation cases of a system entitlement

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.

4. In the **Edit System Entitlement** pane, click the **Attestation** tab.

   This displays all the system entitlement's attestation cases.

5. (Optional) To display more details of an attestation case, click **Details** next to the attestation case.

Related topics

- Attestation on page 101
- Displaying pending attestation cases on page 120

Approving and denying attestation cases of system entitlements

You can grant or deny approval to attestation cases of system entitlements.

To approve an attestation case

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System entitlements**.

3. On the **System Entitlements** page, click the system entitlement whose attestation cases are pending your approval.

4. In the **Edit System Entitlement** pane, click the **Attestation** tab.

5. On the **Attestation** tab, click ▼ (**Filter**).

6. In the filter context menu, under **State**, select the **Pending** option.

7. Perform one of the following actions:

   - To approve an attestation case, in the list, select the check box next to the attestation case and click **Approve** below the list.

   - To deny an attestation case, in the list, select the check box next to the attestation case and click **Deny** below the list.

8. (Optional) In the **Approve Attestation Case** or the **Deny Attestation Case** pane, perform the following actions:

   a. In the **Reason for your decision** field, select a standard reason for your approval decision.

   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

9. Click **Save**.

Related topics

- Attestation on page 101
- Granting or denying attestation cases on page 121

Creating reports about system entitlements

You can create reports on system entitlement data.

To create a report on a system entitlement

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Identities**.

3. On the **System Entitlements** page, click the system entitlement that you want to create a report on.

4. In the **Edit System Entitlement**, click ⋮ (**Actions**) > **Download report**.

Managing departments

You can use the Web Portal to manage departments.

Detailed information about this topic

- Displaying departments on page 247
- Copying/splitting departments on page 249
- Displaying and editing department main data on page 248
- Managing department memberships on page 251
- Managing department entitlements on page 254
- Displaying department rule violations on page 256

Displaying departments

You can see any of the departments and their details.

To display departments

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation click **Departments**.

This opens the **Departments** page and displays all the departments.

3. (Optional) To display details of a department, next to the department, click **Edit**.

Displaying and editing department main data

You can see and edit departments' main data.

To display and edit a department's main data

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department whose main data you want to display, click **Edit**.

4. In the **Edit Department** pane, make your changes in the relevant fields.

Table 34: 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	Select the manager who is responsible for the department.
2nd Manager	Select an identity to act as a deputy to the department's manager.
Additional manager	Click **Assign**/**Change** and select a cost center. Members of the selected application role are responsible for the department.
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.

5. Click **Save**.

Copying/splitting departments

You can copy or move memberships and entitlements from departments you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a department or move memberships and entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department you want to copy or whose memberships and entitlements you want to move, click **Edit**.

4. In the pane, click ⋮ (**Actions**) > **Split**.

5. In the **Split** pane, In the **Type of new role** menu, select which type to give the new object.

6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

   TIP: After the object has been created, you can add the remaining main data (see Displaying and editing my department main data on page 135, Displaying and editing my business roles' main data on page 151, Displaying and editing my cost center main data on page 176, or Displaying and editing my locations' main data on page 184).

7. Click **Continue**.

8. In the **Select assignments to be copied or moved to the new role** step, perform the following actions:

   - To neither copy nor move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep this assignment**. The entitlement/membership is later only available in the source object.

   - To copy or move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new role**. The entitlement/membership is included later in the source object as well as the target object.

   - To move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new role**. The entitlement/membership is later removed from the source object and only included in the target object.

9. Click **Continue**.

10. (Optional) In the **Verify** step, you verify the actions to run and deselect the check box in front of any actions that should not be run.

11. Click **Continue**.

Related topics

- Managing department memberships on page 251
- Managing department entitlements on page 254

Managing department memberships

As soon as an identity is assigned to a department, the identity becomes a member in the department.

Detailed information about this topic

Displaying department memberships

You can display which identities are assigned to certain departments.

To display memberships

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. In the list, next to the department whose memberships you want to display, click **Edit**.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To view all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to departments

You can see how a department assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, next to the department whose memberships you want to display, click **Edit**.
4. In the **Edit Department** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

Adding identities to departments

You can add identities to departments.

The following assignment options are available:

- Assignment by request

- Automatic assignment through a dynamic role

- Revoking exclusion of a member

To assign an identity to a department using a request

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department you want to add an identity to, click **Edit**.

4. In the **Edit Department** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Click **Request memberships**.

7. In the **Select Identities** pane, select the check box next to the identity you want to assign to the department.

8. Click **Request memberships**.

9. Close the **Edit Department** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the department.

To add members automatically through a dynamic role

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department for which you want to create a dynamic role, click **Edit**.

4. In the **Edit Department** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.

6. Click **Create dynamic role**.

7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:

   a. In the **Property** menu, select the relevant property.

   b. In the **Operator** menu, select a logical operator.

   c. In the final field, specify a comparison value.

   d. (Optional) To add another condition, click **Add another condition** and repeat the steps.

   e. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

   TIP: To remove a condition, click 🗑 (**Delete**).

   For more information about customizing filter conditions, see Custom filter conditions.

8. Click **Save**.

9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.

10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.

11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department you want to add again, click **Edit**.

4. In the **Edit Department** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.

7. Click **Remove exclusion**.

Related topics

- Requesting products on page 61

Removing identities from departments

You can remove identities from departments by deleting the corresponding memberships.

To remove a department from an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department with a membership you want to delete, click **Edit**.

4. In the **Edit Department** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

9. If the member was assigned through a dynamic role, perform the following actions:

    a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.

    b. Click **Exclude members**.

Managing 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 254
- Adding entitlements to departments on page 255
- Deleting department entitlements on page 255

Displaying department entitlements

You can see entitlements assigned to departments.

To display entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department whose entitlements you want to display, click **Edit**.

4. In the **Edit Department** pane, click the **Entitlements** tab.

Adding entitlements to departments

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 **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department you want to add an entitlement to, click **Edit**.

4. In the **Edit Department** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, click **Request entitlements**.

6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.

7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.

9. Close the **Edit Department** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    After the request has been granted approval, the entitlement is added to the department.

Related topics

- Requesting products on page 61

Deleting department entitlements

You can delete entitlements assigned to departments.

To delete an entitlement from a department

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department whose entitlement you want to delete, click **Edit**.

4. In the **Edit Department** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.

6. Click **Remove**.

7. Confirm the prompt with **Yes** in the dialog.

Displaying department rule violations

You can see department rule violations.

To display rule violations

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Departments**.

3. On the **Departments** page, next to the department whose rule violations you want to display, click **Edit**.

4. On the **Edit Department** pane, click the **Rule Violations** tab.

Managing locations

You can use the Web Portal to manage locations.

Detailed information about this topic

- Displaying locations on page 256
- Displaying and editing location main data on page 257
- Copying/splitting locations on page 258
- Managing location memberships on page 260
- Managing location entitlements on page 263
- Displaying location rule violations on page 265

Displaying locations

You can see any of the locations and their details.

To display locations

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation click **Locations**.

   This opens the **Locations** page and displays all the locations.

3. (Optional) To display details of a location, next to the location, click **Edit**.

Displaying and editing location main data

You can see and edit locations' main data.

To display and edit a location's main data

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location whose main data you want to display, click **Edit**.

4. In the **Edit Location** pane, make your changes in the relevant fields.

Table 35: 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	Select the manager who is responsible for the location.
2nd Manager	Select an identity to act as a deputy to the location's manager.
Additional manager	Click **Assign**/**Change** and select a cost center. Members of the selected application role are responsible for the location.
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.
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.

5. Click **Save**.

Copying/splitting locations

You can copy or move memberships and entitlements from locations you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a location or move memberships and entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location you want to copy or whose memberships and entitlements you want to move, click **Edit**.

4. In the pane, click ⋮ (**Actions**) > **Split**.

5. In the **Split** pane, In the **Type of new role** menu, select which type to give the new object.

6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

   TIP: After the object has been created, you can add the remaining main data (see Displaying and editing my department main data on page 135, Displaying and editing my business roles' main data on page 151, Displaying and editing my cost center main data on page 176, or Displaying and editing my locations' main data on page 184).

7. Click **Continue**.

8. In the **Select assignments to be copied or moved to the new role** step, perform the following actions:

   - To neither copy nor move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep this assignment**. The entitlement/membership is later only available in the source object.

   - To copy or move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new role**. The entitlement/membership is included later in the source object as well as the target object.

   - To move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new role**. The entitlement/membership is later removed from the source object and only included in the target object.

9. Click **Continue**.

10. (Optional) In the **Verify** step, you verify the actions to run and deselect the check box in front of any actions that should not be run.

11. Click **Continue**.

Related topics

- Managing location memberships on page 260
- Managing location entitlements on page 263

Managing location memberships

As soon as an identity is assigned to a location, the identity becomes a member in the location.

Detailed information about this topic

Displaying location memberships

You can display which identities are assigned to certain locations.

To display memberships

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. In the list, next to the location whose memberships you want to display, click **Edit**.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To view all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to locations

You can see how a location assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, next to the location whose memberships you want to display, click **Edit**.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

Adding identities to locations

You can add identities to locations.

The following assignment options are available:

- Assignment by request

- Automatic assignment through a dynamic role

- Revoking exclusion of a member

To assign an identity to a location using a request

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location you want to add an identity to, click **Edit**.

4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Click **Request memberships**.

7. In the **Select Identities** pane, select the check box next to the identity you want to assign to the location.

8. Click **Request memberships**.

9. Close the **Edit Location** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the location.

To add members automatically through a dynamic role

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location for which you want to create a dynamic role, click **Edit**.

4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.

6. Click **Create dynamic role**.

7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:

a. In the **Property** menu, select the relevant property.

b. In the **Operator** menu, select a logical operator.

c. In the final field, specify a comparison value.

d. (Optional) To add another condition, click **Add another condition** and repeat the steps.

e. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

TIP: To remove a condition, click 🗑 (**Delete**).

For more information about customizing filter conditions, see Custom filter conditions.

8. Click **Save**.

9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.

10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.

11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location you want to add again, click **Edit**.

4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.

7. Click **Remove exclusion**.

Related topics

- Requesting products on page 61

Removing identities from locations

You can remove identities from locations by deleting the corresponding memberships.

To remove a location from an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location with a membership you want to delete, click **Edit**.

4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

9. If the member was assigned through a dynamic role, perform the following actions:

   a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.

   b. Click **Exclude members**.

Managing 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 263
- Adding entitlements to locations on page 264
- Deleting entitlements from locations on page 264

Displaying location entitlements

You can see entitlements assigned to locations.

To display entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location whose entitlements you want to display, click **Edit**.

4. In the **Edit Location** pane, click the **Entitlements** tab.

Adding entitlements to locations

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 **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location you want to add an entitlement to, click **Edit**.

4. In the **Edit Location** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, click **Request entitlements**.

6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.

7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.

9. Close the **Edit Location** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    After the request has been granted approval, the entitlement is added to the location.

Related topics

- Requesting products on page 61

Deleting entitlements from locations

You can delete entitlements assigned to locations.

To delete an entitlement from a location

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location whose entitlement you want to delete, click **Edit**.

4. In the **Edit Location** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.

6. Click **Remove**.

7. Confirm the prompt with **Yes** in the dialog.

Displaying location rule violations

You can see location rule violations.

To display rule violations

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Locations**.

3. On the **Locations** page, next to the location whose rule violations you want to display, click **Edit**.

4. On the **Edit Location** pane, click the **Rule Violations** tab.

Managing cost centers

You can use the Web Portal to manage cost centers.

Detailed information about this topic

- Displaying cost centers on page 265
- Displaying and editing cost center main data on page 266
- Copying/splitting cost centers on page 267
- Managing cost center memberships on page 269
- Managing cost center entitlements on page 272
- Displaying cost center rule violations on page 274

Displaying cost centers

You can see any of the cost centers and their details.

To display cost centers

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation click **Cost centers**.

   This opens the **Cost centers** page and displays all the cost centers.

3. (Optional) To display details of a cost center, next to the cost center, click **Edit**.

Displaying and editing cost center main data

You can see and edit cost centers' main data.

To display and edit a cost center's main data

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center whose main data you want to display, click **Edit**.

4. In the **Edit Cost Center** pane, make your changes in the relevant fields.

Table 36: 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	Select the manager who is responsible for the cost center.
2nd Manager	Select an identity to act as a deputy to the cost center's manager.
Additional manager	Click **Assign**/**Change** and select a cost center. Members of the selected application role are responsible for the department.
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.

5. Click **Save**.

Copying/splitting cost centers

You can copy or move memberships and entitlements from cost centers you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a cost center or move memberships and entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center you want to copy or whose memberships and entitlements you want to move, click **Edit**.

4. In the pane, click ⋮ (**Actions**) > **Split**.

5. In the **Split** pane, In the **Type of new role** menu, select which type to give the new object.

6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

   TIP: After the object has been created, you can add the remaining main data (see Displaying and editing my department main data on page 135, Displaying and editing my business roles' main data on page 151, Displaying and editing my cost center main data on page 176, or Displaying and editing my locations' main data on page 184).

7. Click **Continue**.

8. In the **Select assignments to be copied or moved to the new role** step, perform the following actions:

   - To neither copy nor move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep this assignment**. The entitlement/membership is later only available in the source object.

   - To copy or move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new role**. The entitlement/membership is included later in the source object as well as the target object.

   - To move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new role**. The entitlement/membership is later removed from the source object and only included in the target object.

9. Click **Continue**.

10. (Optional) In the **Verify** step, you verify the actions to run and deselect the check box in front of any actions that should not be run.

11. Click **Continue**.

Related topics

- Managing cost center memberships on page 269
- Managing cost center entitlements on page 272

Managing cost center memberships

As soon as an identity is assigned to a cost center, the identity becomes a member in the cost center.

Detailed information about this topic

- Displaying cost center memberships on page 269
- Analyzing assignments to cost centers on page 269
- Adding identities to cost centers on page 270
- Removing identities from cost centers on page 271

Displaying cost center memberships

You can display which identities are assigned to certain cost centers.

To display memberships

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. In the list, next to the cost center whose memberships you want to display, click **Edit**.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To view all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to cost centers

You can see how a cost center assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, next to the cost center whose memberships you want to display, click **Edit**.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

Adding identities to cost centers

You can add identities to cost centers.

The following assignment options are available:

- Assignment by request
- Automatic assignment through a dynamic role
- Revoking exclusion of a member

To assign an identity to a cost center using a request

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center you want to add an identity to, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Click **Request memberships**.

7. In the **Select Identities** pane, select the check box next to the identity you want to assign to the cost center.

8. Click **Request memberships**.

9. Close the **Edit Cost Center** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the cost center.

To add members automatically through a dynamic role

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Cost centers**.

3. On the **Cost centers** page, next to the cost center for which you want to create a dynamic role, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.

6. Click **Create dynamic role**.

7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:

   a. In the **Property** menu, select the relevant property.

   b. In the **Operator** menu, select a logical operator.

   c. In the final field, specify a comparison value.

   d. (Optional) To add another condition, click **Add another condition** and repeat the steps.

   e. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

   TIP: To remove a condition, click 🗑 (**Delete**).

   For more information about customizing filter conditions, see Custom filter conditions.

8. Click **Save**.

9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.

10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.

11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center you want to add again, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.

7. Click **Remove exclusion**.

Related topics

- Requesting products on page 61

Removing identities from cost centers

You can remove identities from cost centers by deleting the corresponding memberships.

To remove a cost center from an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center with a membership you want to delete, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

9. If the member was assigned through a dynamic role, perform the following actions:

   a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.

   b. Click **Exclude members**.

Managing 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 272
- Adding entitlements to cost centers on page 273
- Deleting cost center entitlements on page 273

Displaying cost center entitlements

You can see entitlements assigned to cost centers.

To display entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center whose entitlements you want to display, click **Edit**.

4. In the **Edit Cost Center** pane, click the **Entitlements** tab.

Adding entitlements to cost centers

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 **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, next to the cost center you want to add an entitlement to, click **Edit**.
4. In the **Edit Cost Center** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.
9. Close the **Edit Cost Center** pane.
10. In the menu bar, click **Requests** > **Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

    After the request has been granted approval, the entitlement is added to the cost center.

Related topics

- Requesting products on page 61

Deleting cost center entitlements

You can delete entitlements assigned to cost centers.

To delete an entitlement from a cost center

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, next to the cost center whose entitlement you want to delete, click **Edit**.
4. In the **Edit Cost Center** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying cost center rule violations

You can see cost center rule violations.

To display rule violations

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Cost centers**.

3. On the **Cost Centers** page, next to the cost center whose rule violations you want to display, click **Edit**.

4. On the **Edit Cost Center** pane, click the **Rule Violations** tab.

Managing business roles

You can use the Web Portal to manage business roles.

Detailed information about this topic

- Displaying business roles on page 274
- Displaying and editing business role main data on page 275
- Copying/splitting business roles on page 277
- Managing business role memberships on page 278
- Managing business role entitlements on page 281
- Displaying business role rule violations on page 283

Displaying business roles

You can see any of the business roles and their details.

To display business roles

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation click **Business roles**.

   This opens the **Business Roles** page and displays all the business roles.

3. (Optional) To view details of a business role, next to the business role, click **Edit**.

Displaying and editing business role main data

You can see and edit the system roles' main data.

To display and edit a business role's main data

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role whose main data you want to display, click **Edit**.

4. In the **Edit Business Roles** pane, make your changes in the relevant fields.

Table 37: 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	Select the manager who is responsible for the business role.
2nd Manager	Select an identity to act as a deputy to the business role's manager.
Additional manager	Click **Assign**/**Change** and select a cost center. Members of the selected application role are responsible for the department.
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.

5. Click **Save**.

Copying/splitting business roles

You can copy or move memberships and entitlements from business roles you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a business role or move memberships and entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role you want to copy or whose memberships and entitlements you want to move, click **Edit**.

4. In the pane, click ⋮ (**Actions**) > **Split**.

5. In the **Split** pane, In the **Type of new role** menu, select which type to give the new object.

6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

   TIP: After the object has been created, you can add the remaining main data (see Displaying and editing my department main data on page 135, Displaying and editing my business roles' main data on page 151, Displaying and editing my cost center main data on page 176, or Displaying and editing my locations' main data on page 184).

7. Click **Continue**.

8. In the **Select assignments to be copied or moved to the new role** step, perform the following actions:

   - To neither copy nor move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep this assignment**. The entitlement/membership is later only available in the source object.

   - To copy or move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new role**. The entitlement/membership is included later in the source object as well as the target object.

   - To move an entitlement/a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new role**. The entitlement/membership is later removed from the source object and only included in the target object.

9. Click **Continue**.

10. (Optional) In the **Verify** step, you verify the actions to run and deselect the check box in front of any actions that should not be run.

11. Click **Continue**.

Related topics

Managing business role memberships

As soon as a business role is assigned to an identity, the identity becomes a member in the business role.

Detailed information about this topic

Displaying business role memberships

You can display which identities are assigned to certain business roles.

To display memberships

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. In the list, next to the business role whose memberships you want to display, click **Edit**.
4. In the **Edit Business Roles** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To view all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to business roles

You can assign business roles to identities. The business role is then assigned through a request by displaying an assignment analysis for the corresponding membership.

You can see how a business role assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role whose memberships you want to display, click **Edit**.

4. In the **Edit Business Roles** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

Assigning identities to business roles

You can assign business roles to identities.

The following assignment options are available:

- Assignment by request
- Automatic assignment through a dynamic role
- Revoking exclusion of a member

To assign an identity to a business role using a request

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role you want to add an identity to, click **Edit**.

4. In the **Edit Business Roles** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Click **Request memberships**.

7. In the **Select Identities** pane, select the check box next to the identity you want to assign to the business role.

8. Click **Request memberships**.

9. Close the **Edit Business Roles** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the business role.

To add members automatically through a dynamic role

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role for which you want to create a dynamic role, click **Edit**.

4. In the **Edit Business Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.

6. Click **Create dynamic role**.

7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:

   a. In the **Property** menu, select the relevant property.

   b. In the **Operator** menu, select a logical operator.

   c. In the final field, specify a comparison value.

   d. (Optional) To add another condition, click **Add another condition** and repeat the steps.

   e. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

   | TIP: To remove a condition, click 🗑 (**Delete**).

   For more information about customizing filter conditions, see Custom filter conditions.

8. Click **Save**.

9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.

10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.

11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role you want to add again, click **Edit**.

4. In the **Edit Business Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.

7. Click **Remove exclusion**.

Related topics

- Requesting products on page 61

Removing business roles from identities

You can remove identities from business roles by deleting the corresponding memberships.

To remove a business role from an identity

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, next to the business role with a membership you want to delete, click **Edit**.
4. In the **Edit Business Roles** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.
6. Select the check box next to the membership you want to delete.
7. Click **Remove**.
8. In the **Remove Memberships** pane, click **Remove memberships**.
9. If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.
   b. Click **Exclude members**.

Managing 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 281
- Adding entitlements to business roles on page 282
- Deleting business role entitlements on page 282

Displaying business role entitlements

You can see entitlements assigned to business roles.

To display entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role whose entitlements you want to display, click **Edit**.

4. In the **Edit Business Role** pane, click the **Entitlements** tab.

Adding entitlements to business roles

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 **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role you want to add an entitlement to, click **Edit**.

4. In the **Edit Business Role** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, click **Request entitlements**.

6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.

7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.

9. Close the **Edit Business Role** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

    After the request has been granted approval, the entitlement is added to the business role.

Related topics

- Requesting products on page 61

Deleting business role entitlements

You can delete entitlements assigned to business roles.

To delete an entitlement from a business role

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role whose entitlement you want to delete, click **Edit**.

4. In the **Edit Business Role** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.

6. Click **Remove**.

7. Confirm the prompt with **Yes** in the dialog.

Displaying business role rule violations

You can see business role rule violations.

To display rule violations

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **Business roles**.

3. On the **Business Roles** page, next to the business role whose rule violations you want to display, click **Edit**.

4. On the **Edit Business Role** pane, click the **Rule Violations** tab.

Managing system roles

You can use the Web Portal to manage system roles.

Detailed information about this topic

Displaying system roles

You can see any of the system roles and their details.

To display system roles

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation click **System roles**.

   This opens the **System Roles** page and displays all the System roles.

3. (Optional) To display details of a system role, click **Edit** next to the system role.

Displaying and editing system role main data

You can see and edit the business roles' main data.

To display and edit a system role's main data

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System roles**.

3. On the **System Roles** page, next to the system role whose main data you want to display, click **Edit**.

4. In the **Edit System Role** pane, make your changes in the relevant fields.

Table 38: 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	Shows you the associated service item.
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.

5. Click **Save**.

Managing system role memberships

As soon as a system role is assigned to an identity, the identity becomes a member in the system role.

Detailed information about this topic

-
-
-
-

Displaying system role memberships

You can display which identities are assigned to certain system roles.

To display memberships

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. In the list, next to the system role whose memberships you want to display, click **Edit**.
4. In the **Edit System Role** pane, click the **Memberships** tab.

Analyzing assignments to system roles

You can see how a system role assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, next to the system role whose memberships you want to display, click **Edit**.
4. In the **Edit System Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, select the check box next to the corresponding membership.
6. Click **View assignment analysis**.

Assigning identities to system roles

You can assign system roles to identities. You do this through requests.

To assign an identity to a system role using a request

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System roles**.

3. On the **System Roles** page, next to the system role you want to add an identity to, click **Edit**.

4. In the **Edit System Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Request memberships**.

6. In the **Select Identities** pane, select the check box next to the identity you want to assign to the system role.

7. Click **Request memberships**.

8. Close the **Edit System Role** pane.

9. In the menu bar, click **Requests** > **Shopping cart**.

10. On the **Shopping Cart** page, click **Submit**.

    Once the request has been granted approval, the identity is assigned to the system role.

Related topics

- Requesting products on page 61

Removing identities from my system roles

You can remove identities from system roles by deleting the corresponding memberships.

To remove a system role from an identity

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System roles**.

3. On the **System Roles** page, next to the system role with a membership you want to delete, click **Edit**.

4. In the **Edit System Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary Memberships**.

6. Select the check box next to the membership you want to delete.

7. Click **Remove**.

8. In the **Remove Memberships** pane, click **Remove memberships**.

Managing 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 288
- Adding entitlements to system roles on page 288
- Deleting system role entitlements on page 289

Displaying system role entitlements

You can see entitlements assigned to system roles.

To display entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, next to the system role whose entitlements you want to display, click **Edit**.
4. In the **Edit System Role** pane, click the **Entitlements** tab.

Adding entitlements to system roles

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 **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, next to the system role you want to add an entitlement to, click **Edit**.
4. In the **Edit System Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add**, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.

9. Close the **Edit System Role** pane.

10. In the menu bar, click **Requests** > **Shopping cart**.

11. On the **Shopping Cart** page, click **Submit**.

   After the request has been granted approval, the entitlement is added to the system role.

Related topics

- Requesting products on page 61

Deleting system role entitlements

You can delete entitlements assigned to system roles.

To delete an entitlement from a system role

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System roles**.

3. On the **System Roles** page, next to the system role whose entitlements you want to display, click **Edit**.

4. In the **Edit System Role** pane, click the **Entitlements** tab.

5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.

6. Click **Remove**.

7. Confirm the prompt with **Yes** in the dialog.

Displaying system role rule violations

You can see system role rule violations.

To display rule violations

1. In the menu bar click **Data administration** > **Data Explorer**.

2. In the Data Explorer navigation, click **System roles**.

3. On the **System Roles** page, next to the system role whose rule violations you want to display, click **Edit**.

4. On the **Edit System Role** pane, click the **Rule Violations** tab.

ONE IDENTITY
by Quest

Appendix: Attestation conditions and approval policies from attestation procedures

When attestation policies are created or edited (see Setting up attestation policies on page 104 or Editing attestation policies on page 106), 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 depart-ments	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

Condition	Description
	department are attested.
	Use ⬍ and ☰ to switch between hierarchical and list view. Multi-select is possible.
Departments with defined risk index	Use the **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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

ONE IDENTITY by Quest

One Identity Manager 9.1 Web Portal User Guide
Appendix: Attestation conditions and approval policies from attestation procedures

294

Condition	Description
	possible.
Locations with defined risk index	Use the **Lower limit** and **Upper limit** fields to define 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.

ONE IDENTITY
by Quest

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.

ONE IDENTITY
by Quest

One Identity Manager 9.1 Web Portal User Guide
Appendix: Attestation conditions and approval policies from attestation procedures

296

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

ONE IDENTITY
by Quest

One Identity Manager 9.1 Web Portal User Guide
Appendix: Attestation conditions and approval policies from attestation procedures

298

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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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:

ONE IDENTITY
by Quest

One Identity Manager 9.1 Web Portal User Guide
Appendix: Attestation conditions and approval policies from attestation procedures

301

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 **Lower limit** and **Upper limit** fields to define 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 Certification of business roles	Business role managers can make approval decisions through attestation cases. 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	Select the cost centers to attest.

Condition	Description
centers	Use ⤵ and ☰ to switch between hierarchical and list view. Multi-select is possible.
Cost centers with defined risk index	Use the **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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.

Approval policies	Description
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.

Condition	Description
System entitlements with specific owners	Select the identities. Attests memberships in system entitlements that are managed by these identities.
System entitlements in a target system container	Select the target system containers. Attests memberships in system entitlements found in these target system containers.
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 **Lower limit** and **Upper limit** fields to define 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 attestation 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 117)
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.

Condition	Description
	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: • **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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 assign-ment 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 entitlements	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).

ONE IDENTITY
by Quest

One Identity Manager 9.1 Web Portal User Guide
Appendix: Attestation conditions and approval policies from attestation procedures

312

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All system entitlements 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	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	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 entitlements by applications	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 entitlements	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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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.

Condition	Description
System entitlements with defined risk index	Use the **Lower limit** and **Upper limit** fields to define a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to business roles.
System entitlements 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 entitlements	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 **Lower limit** and **Upper limit** fields to define a risk index range. Attests system entitlement assignments to cost centers with a risk index in the chosen range.

ONE IDENTITY
by Quest

One Identity Manager 9.1 Web Portal User Guide
Appendix: Attestation conditions and approval policies from
attestation procedures

318

Condition	Description
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 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 **Lower limit** and **Upper limit** fields to define 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.

ONE IDENTITY
by Quest

One Identity Manager 9.1 Web Portal User Guide
Appendix: Attestation conditions and approval policies from attestation procedures

319

Condition	Description
	Use ⇅ and ☰ to switch between hierarchical and list view. Multi-select is possible.
Specific system entitlements	Select the with system entitlements with assignments to locations to attest.
Locations with defined risk index	Use the **Lower limit** and **Upper limit** fields to define 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 entitlements with defined risk index	Use the **Lower limit** and **Upper limit** fields to define a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to locations.
System entitlements 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	Select an attestation status Attests assignments of system roles, matching this attestation status, to departments.

Condition	Description
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 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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	Attests assignments of system roles to all business roles.

Condition	Description
roles	
All system roles	Attests assignments of all system roles to business roles.
Attesting by attestation status	Select an attestation status Attests assignments of system roles, 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define 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 **Lower limit** and **Upper limit** fields to define a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to cost centers.
System roles with matching name	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 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 **Lower limit** and **Upper limit** fields to define 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 with defined risk index	Use the **Lower limit** and **Upper limit** fields to define a risk index range. Attests assignments of 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 applic- ations	Select the applications. Attests assignments to system roles assigned to these applications.
System roles with defined risk index	Use the **Lower limit** and **Upper limit** fields to define 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.

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