Dell™ One Identity Manager 7.1.3

Web Portal User Guide

Legend

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

⚠ | **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

ⓘ | **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Contents

Getting Started with the One Identity Manager Web Portal

The standard Web Portal is part of an internet application which you can use from your internet browser. The prerequisite for this is a correctly configured Web server and a One Identity Manager database configured and populated with user data. Using the standard Web Portal, you can request and cancel products, as well as renew limited requests. Authorized employees can approve requests and cancellations, perform attestations, view rule violations and grant or deny exception approval. Furthermore, you can change the main password and generate statistics.

Depending on your role and level of security, you can use the Web Portal to:

- Request access to resources
- Track the progress of your requests
- Approve or deny requests made by your employees
- Subscribing reports
- Manage rule violations
- View reports and statistics on resources or roles assigned to you or your employees

The standard Web Portal can be used without restrictions if the following guidelines are taken into account.

Table 1: Supports browser for the desktop and mobile Web Portal view.

Browser	Windows	MacOSCX	IOS	Android	Windows Phone (SF)
Internet Explorer®	Version 10.0 or later				Current version
Firefox®	(Release Channel)			Current version	
Chrome™	(Release Channel)			Current version	
Safari®		Current version	Current version		
Microsoft® Edge	(Release Channel)				(Release Channel)

ⓘ **NOTE:** Enable JavaScript in your browser to allow full usage of the Web Portal.

ⓘ **NOTE:** Other browsers may have reduced functionality, or may not perform as expected.

ⓘ **NOTE:** Use the Web Installer program to set up Internet Information Services and to publish the One Identity Manager standard Web Portal. You can find instruction for this program in the Dell One Identity Manager Installation Guide.

The following software must be available on the server:

- Apache™ 2.0 or 2.2 with following modules:mod_mono, rewrite, ssl (optional)

- Mono® version 4.6 or later

- Internet Information Services version 7 and

- Microsoft® .NET Framework version 4.5.2 or 4.6.1

Table 2: Additional System Requirements for Implementing an Oracle Database

Additional software	Windows® operating system
	- Oracle Client Tools This version should correspond at least to the version of the database in use. Note the recommendation of Oracle with respect to the Client Tools you want to implement. In a 64-bit system the Oracle clients are required in 64-bit and 32-bit versions. ⓘ **NOTE:** Use of Oracle Client Tools is only supported by Web Designer under Windows® operating systems. ⓘ **NOTE:** If a direct connection is possibleOracle to the database by TCP/IP, the client is not Oraclenecessary. The Oracle connector integrated in Web Designer sets up the database connection. ⓘ **NOTE:** Use of Oracle® Real Application Clusters and other Oracle database configurations, which either require - input of several "ADDRESS" entries for one "net_service_name" in the client-side `tnsnames.ora` or - additional entries in the client-side `sqlnet.ora` have access to the Oracle database through the Oracle client.

ⓘ **NOTE:** The standard Web Portal is supplied in German and English. You merely have to load the corresponding translations for this. All operations with the One Identity Manager standard Web Portal is preceded by authentication. Possible authentication methods concur with the methods used for all other One Identity Manager tools. Some authentication methods allow single sign on, making it possible for you to log in without having to enter authentication data every time.

A minimum screen resolution of 1280 x 1024 pixels is recommended with at least 16 bit color in order to optimize the user interface graphics. A display size of at least 9.7 inches is recommended for mobile displays, for example, when using a tablet.

Logging On and Off

You must be logged onto the system to be able to work with the Web Portal. If you do not have an account, you can request one for using 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.

ⓘ **NOTE:** You can configure and extend the standard Web Portal with the Web Designer.

To log onto the system for the first time

1. Open the Web Portal login page by entering the Web Portal URL in the browser's address bar.

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

2. Click **New account**.

3. Fill out **First name** and **Last name** as a minimum.

4. Enter the CAPTCHA code in the box, or select a new CAPTCHA code if necessary.

5. Click **Save** to confirm.

   A message appears indicating that your account has been added. Take note of your user name and email address. Once your account has been confirmed by the manager responsible, you will receive notification by email with the required login information.

To connect to the Web Portal

1. Type the Web Portal URL in the address bar to Open the Web Portal page.

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

2. Enter your complete login name in **Login name**.

3. Enter your password in **Password**.

4. Change the language if required.

   ⓘ **NOTE:** You have the option to run the Web Portal in different languages. English and German are supplied by default.

5. Click **Log in**.

   ⓘ **TIP:** Have you forgotten your password? Click **Forgot your password?**. This takes you to the Dell™ One Identity Password Manager self-help page. For more information about resetting your password, see the One Identity Password Manager.

To log off the Web Portal

1. Click on your user name in the header and then **Log off**.

2. Confirm with **Yes**.

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

Updating your Contact Information

Once you have logged in to the system for the first time, or any time you move within the company, you should update your contact information.

ⓘ **NOTE:** Light gray text boxes cannot be edited.

To update your contact information

1. Click on the user name in the header and then **My settings**.

    The tab **Contact Data** is preselected.

    ⓘ | **NOTE:** A user, with other sub identities apart from a main identity in the Web Portal, can select an identity from the **Identity** menu on the **Contact Data** tab.

    Changes to their contact data only affects the selected identity.

    This also applies to creating reports. If you create a report it is generated for the selected identity.

2. Select the text you want and add or correct the details.

3. Click **Assign** next to the **Country** link and perform one of the following tasks.

    a. Select the country you want from the list.

    b. Click the filter to limit your search to the desired country.

4. Click 🖊 next to **Picture**.

    This opens the dialog box **Picture**.

    ⓘ | **NOTE:** You may have the option to change your picture depending on the configuration and your permissions.

5. Click **Browse...** to search for a picture and confirm your selection with **Apply**.

    The selected image and other instruction are displayed in the dialog box. If the image is larger that 10KB, you must crop it.

6. Hold the mouse over the image until a cross cursor appears, click with the left mouse button and drag the mouse diagonally down over the image until the you have selected the required area.

7. Crop the photo with **Crop to selection** and save the cut with **Apply**.

8. Click **Save** on the **Contact Data** tab to save your changes.

To edit your Active Directory® user accounts

1. Click on the user name in the header and then **My settings**.

2. Select the **Active Directory® user accounts** tab.

3. Enable the Active Directory® user account you want, if there are more than one.

4. Edit the text boxes or add new ones.

5. Save the changes.

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

Configuring up your Web Portal Language Settings

You can configure which language you want use in the Web Portal.

To set the language for your web application

1. Click on the user name in the header and then **My settings**.

   The tab **Contact Data** is preselected.

2. Click **Change** next to the **Language** entry and select your preferred language.

3. Save the changes.

   The changes take effect immediately in the Web Portal.

ⓘ **NOTE:** Another way of changing the language is through the browser. The browser settings only apply if your web application does not specify a language.

Navigating around the Web Portal

Once you have logged in, you can use the Web Portal to view and manage your information.

ⓘ **NOTE:** The Web Portal is customized for you, based on your organization's implementation of the solution, and your role in the organization. Which groups of employees are supplied with which functionality in the standard installation is explained in the following chapters.

You have three main menus in the Web Portal. The following are available:

- My Identity
- Access Governance
- Governance Administration

The menu **My Identity** contains functions relating the current user's tasks. The functions might be business instances, responsibilities or employee to be accounted for.

The menu **Access Governance** provides you with functions for (company wide) data analysis. Here, specially entitled people can view data and statistics on the topics **Compliance**, **Attestation**, **Risk**.

The menu **Governance Administration** provides system administration functionality.

To select a main menu

1. Click ▾ in the header above the menu bar.

   A menu is displayed showing the main menus available to you.

2. Select the menu you want.

Exploring Your Home Page

Once you have logged in successfully, the home page appears. The home page consists of the following components:

- Header

  The header is at the top of screen next to the company logo. You can call up a view from here with you personal data, memberships, responsibilities and entitlements.

- Breadcrumb Navigation

  Breadcrumb navigation shows you the path you have taken to get to your current location. Use the **Start** button to return to the home page. Users who use a reading program to operate the Web Portal, can go directly to the navigation by using an invisible link, which is in the header section of every page.

- Menu bar

  The menu bar is displayed on the left-hand side of the screen and provides different menus and submenus.

- Main Content Page

  The main content of the start page is divided into two parts (frames).

Detailed information about this topic

Using the Main Navigation

On the left-hand side of the screen you will see the main navigation menu. Each menu can be expanded to see the available functions. At any time, you can click Start to return to the home page.

ⓘ **NOTE:** The menu items you see depend on the system configuration and your access permissions. For more information about granting entitlements, see the Dell One Identity Manager Web Designer Reference Guide and for configuring components, the Dell One Identity Manager Configuration Guide.

The following table shows which people have access to each of menus. Prerequisite for this is that the QER\IT Shop configuration parameter is set. This configuration parameter is set and the IT Shop is available, by default. If the configuration parameter is not set, you can set it in the and then compile the database.Designer For more detailed information, see the .Dell One Identity Manager Configuration Guide

ⓘ **NOTE:** Which menu items you see, depends on the main menu you selected. For more information, see Navigating around the Web Portal on page 12.

The following tables show the menu items belonging to the main menus **My Identity**, **Access Governance** and **Governance Administration**. You can always select the menu item **My Profile** in the header.

Table 3: Visible menus - header

Menu items	Employees	Manager /Supervisor	External Auditor
My Profile	Yes	Yes	

Table 4: Visible menus - main menu "My Identity"

Menu items	Employees	Manager /Supervisor	External Auditor
My Actions	Yes	Yes	
My Business Ownerships		Yes	

Menu items	Employees	Manager /Supervisor	External Auditor
My Action History	Yes	Yes	
Service catalog	Yes	Yes	

Table 5: Visible menus - main menu "Access Governance"

Menu items	Employees	Manager /Supervisor	External Auditor
Compliance		Yes	
Auditing		Yes	Yes

Table 6: Visible menus - main menu "Governance Administration"

Menu items	Employees	Manager /Supervisor	External Auditor
Administrator		Yes	Yes
Governed Data		Yes	Yes

Making Approval Decisions about Pending Items

If you can see a number displayed beside **My Actions**, it represents the sum of all pending items for which you are responsible and which require an approval decision from you. These items are displayed in submenus under **My Actions** and on the main content page on the right below bookmarks. If there is a number next to the submenu, your action is required. This might mean, for example, that you must grant or deny approval to pending requests. Pending items are normally, requests, inquiries or attestations.

To make approval decisions about pending items

1. Open a submenu under **My Actions**, which has a number after it.

    This opens a view displaying the pending items.

2. Perform one of the following tasks.

    a. Grant approval for an item by clicking on ☑.

    b. Deny approval for an item by clicking on ☒.

3. Perform one of the following tasks.

    a. Continue as in step 2.

    b. Click **Next** and **Save approvals** in the **Approvals** view.

        The number next to the menu item with the pending item is either decreased or no longer displayed.

Main Sections

The start page of the main content page **My Identity** provides you with an overview of your tasks and the products you can request. This part of the start page is principally divided into two parts. This sections are:

- Service catalog

  In this section you will find service categories from which you can make requests. Your access rights and permissions determine your selection of service categories. You can click on a category to got to the request page. On the request page, you can see the products belonging to the selected service category.

- Responsibilities

  This section shows you different statistics of responsibilities. You can click on each statistic. You can find statistics, which you cannot immediately see, on the start page by clicking the arrow on the right-hand side.

- Bookmarks

  On the right-hand side of the main content page you can see a list of bookmarks you have set, amongst other things. You can click on these products or tasks to navigate to the corresponding page for more editing or to delete them from the list by using **Delete**.

- Pending Requests

  This section is also on the right-hand side of the main content page. You can see the last 5 transacted pending requests and click on them. Using the link **View all pending requests**, you navigate to the page with all pending requests.

- Pending Attestations

  This section is also on the right-hand side of the main content page. You can see the last 5 transacted pending attestations and click on them. Using the link **View all pending attestations**, you navigate to the page with all pending attestations.

The **Access Governance** main content page displays the following section assuming you have sufficient viewing permissions.

- Compliance

  The Manager can be used to define rules that maintain and monitor regulatory requirements and automatically deal with rule violations. Rules are used for locating rule violations and to prevent them.

- Risk

  Many items have a risk index associated with them, allowing the Manager to make a risk assessment. You can view which factors contribute to the assessment of the selected object.

- Policies

  Here you will find information about policies and policy violations.

- Organizations

  Here you obtain information about departments in your area of responsibility like employee accounts, employees, rule violations, pending request and the top 10 entitlements and roles.

- IT Shop

  The IT Shop is the tool employees use to make requests. Here you will find information about the popularity and the owners of a product. In addition, you can discover how quickly requests were handled and how often the products were requested.

- attestation

  Attestation polices determine which objects require attestation, by whom, and how often.

- Target systems

  Here you can view which employees assigned in the Manager have access to network resources.

The **Governance Administration** main content does not have a start page. You will find the following menus:

- Risk Assessment

  This menu item lists risk index functions. You can view these and edit them. Risk assessment is a submenu of the **Administration** menu.

- Attestation Policies

  Here you see a list of attestation runs and can change the execution date or sent reminders. In another list, you view and edit attestation policies or add new ones. Attestation policies are another submenu of the **Administration** menu.

- The menu **Identity Management** offers a submenus **Organization** and **Business Roles**. You can use these menus to restore deleted role and edit them.

- Under the menu **Target systems**, you will find the submenu **System Entitlements** .

Icons for Navigating in the Web Portal

There are several buttons available to you in the Web Portal's header bar, which make it easier and simpler to access functions and settings. This following table lists the buttons and explains which functions and settings they call up.

Table 7: Icons in the Web Portal's Header

Icon	Function

👤	The user's name is displayed beside this icon and when you click on 👤, a context menu opens with more menu items. You can select the following menu items:
	
	   • My Profile
	   • My Settings
	   • Log off
	
	When you select **My Profile** you switch to the **Overview**, which displays your personal data along with your memberships, responsibilities and entitlements.
	
	Use the **My Settings** menu item to access the **My Settings** view with the personal data that you can view and edit. This view contains other tabs that you can use to configure your email notification and report settings.
	
	Use the **Log Off** to exit the Web Portal.

🛒	The number of requests that you have still have in your cart appear next to this icon. Click 🛒 to open your cart and submit requests. For more information, see Using your Shopping Cart to Submit your Requests on page 44.
🔖	This icon is displayed in the header if you added bookmarks in the Web Portal. If you see 🔖 in the header, you can click on it and select on the bookmarks to open the respective page. For more information, see Working with Bookmarks on page 23.

Icon	Function
(info icon)	Use this icon to open the **Info** menu with the following menu items: • White Pages • Help • Connection • Switch to mobile view* • Info * This menu item is called "Switch to desktop view" in the mobile view. Use the **White Pages** item to open the company address book. Use **Help** to open the context-sensitive help. The help contains the entire contents of the Web Portal User Guide. The **Connection** menu item opens a dialog box with detailed information about your web application connection. The information is divided into the tabs **System users**, **Permissions groups** and **Program functions**. The **Switch to mobile view** takes you to the Web Portal's mobile view. For more information, see Switching Between the Mobile and Desktop Views on page 31.

Easy Navigation with Keyboard Shortcuts and Help Keys

Simple Commands

Table 8: 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. The shortcuts described here were set up with the help of Internet Explorer® 9.

Go to start page

Table 9: Overview of key combinations for navigating

TAB	Navigate forward.
SHIFT + TAB	Navigate backward.
ENTER	Execute an action.

The elements on the home page are selected in the following order.

1. One Identity Manager logo (link to start page).

2. Dell logo.

3. Settings in the heading.

4. Menu left side.

5. Different categories.

You can recognize the selected element by the outline or underline.

Search	You can use the tab key to select the **Search** box. Once the box is selected, the search entry disappears and you can enter a new term in **Search**. Confirm your input with ENTER.

Simple Elements

Table 10: Overview of the controls used

Button	Use the tab key to navigate to the control and press ENTER to execute the action.
Link	Navigate to the desire link with TAB and press ENTER to open a new page or dialog box.
Popup	Click ESC to leave the popup window with executing anything. Click ENTER to execute. If there is more than one action to execute, navigate with TAB to the desired action and execute with ENTER.
Menu	Use TAB to navigate to the menu. The selected element changes its color. Press **ALT + DOWN-ARROW** or **ALT + UP-ARROW** 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.
Text box	Navigate to the desired text box. If text input is possible, the cursor blinks and you can write in the text box. Exit the text box with TAB. You do not need to confirm by pressing ENTER or SPACE.
Tab	Navigate to the desired tab and press ENTER to display the contents.
Check box	If a check box is already enabled, it means it has been preset. Use SPACE to select the desired check box. You can multi-select.
Radio button	Use radio buttons to enable a function or to make a selection. Use SPACE to select a radio button. Multi-select is not available.

Installed Controls

Table 11: Overview of other controls

Tree view	Use ENTER to expand or collapse a tree view. A plus sign next to the tree root mean it can be expanded by pressing ENTER. A minus sign means it can be collapsed by pressing ENTER.
Calender	Navigate to the arrow next to the date display and use SPACE to open the calender. Today's date is grayed out. Navigate with TAB to set the month and year. Use CTRL + ENTER to select a day.

Tips for using the Web Portal

You can search, sort and filter information in the Web Portal before you display it in a view. If your view is a Hyper View, you can move shapes to any position you want to optimize your view. The same functions are available in many overviews, result lists and information elements. These are described in more detail in the following table.

How to Search

A lot of views provide the option to search by the current context. For example, when you look at your list of resources, you can search specifically for one resource. You can select the simple search, where you enter a single search string, or the advanced search, where you can apply several parameter to the search.

ⓘ | **NOTE:** The searches are not case sensitive.

However, there are certain rules that make successful global searching possible in the Web Portal. These are described in the following table using examples.

Table 12: Rules with examples for searching in the Web Portal

Example	Description
John Doe	Finds John Doe but nor John Donut.
	Search results must contain ALL of the separate terms in the query. A logical "AND" is applied.
John OR Doe	Finds Jane Doe and John Donut.
	Adding an "OR" between the search terms, acts as a logical OR operator. The result of this search contain at least one of the two search terms.
John NOT Doe	Finds John but not John Doe.
	Results of this search do not contain the term, which comes after "NOT".
J*	Finds John and Joanna.
	The * is a wildcard for any other characters, which complete the term.
Do?	Finds Doe but not Donut.
	The ? is a wildcard for one more character, which completes the term.
"John Doe"	Finds results in which "John" and "Doe"
	Results of this search contain the string in quotes as phrase.
John Doe~	Finds Jon Does but also other similar results. A tilde after the search term, allows the search to find similar results. The 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.

To display the search results to the user as quickly as possible, suggestions for possible words are already shown for while you are entering the characters. This includes the final word you enter, if it is not ended by a delimiter. This behavior applies if the project parameter `VI_Common_SqlSearch_PrefixLike` is set.

During the search, the search strings are broken down into tokens by the search index in use. The search terms are compared with these tokens.

Tokens are generally broken down by separating at spaces and also round brackets, square brackets and commas, whereby these characters are omitted. You can define delimiters in the configuration parameter `Common\Indexing\IndexNonTokenChars`.

The configuration parameter `Common\Indexing\IndexNonTokenChars` can be extended if certain characters in the search text have linking function.

There is still alternative tokenizing that is used if the configuration parameter `Common\Indexing\IndexUseLegacyAnalyzer` is set.

ⓘ **NOTE:** The alternative method of tokenizing is preferable for long tokens. For example, if the string "Department_01" is a token, the partial string "Department" is considered to be a token.

ⓘ **NOTE:** Changing the configuration parameter means rebuilding the search index, which may take some time.

The following tokens are named.

Table 13: Tokens for alternative tokenizing

Token	Description with Example
Words	Sequence of letters and/or numbers
Enumeration	Words linked by punctuation marks (_-/.,) of which at least every second one contains a number.
	An example is Department_01.
	Sequences are also decimal numbers and IP addresses.
Email Addresses	An email address is often made up of first name, last name, company name and generic top-level domain (for example .com). The order or spelling of the first and last names may vary (for example, use of initials). The special character @ and the punctuation mark . not only separate each part of the email address but also links them so that the email address is acknowledged as a token.
	Examples of email addresses are Ben.King@company.com or C.Harris@company.com.
Host names	For example, website.xyz.com
Acronym	For example, U.S.A.
Apostrophe	For example, O'Reilly
@, & surrounded by letters	For example, Me&you.
Umlauts such as ä, ö, ü	For example, Max Müller.

To execute a context independent search.

ⓘ **NOTE:** Context independent help is available everywhere in the Web Portal.

1. Click 🔍 in the breadcrumb navigation and enter the search term.
2. Press **Enter**.

   This shows the search results in the main content view.

To execute a simple search

ⓘ **NOTE:** You will find the simple search everywhere where there are more than one items listed.

- Perform one of the following tasks.
  a. Mark one of the entries in the list.
  b. Apply a filter before you mark an entry in the result list.

For more information, see Using a Filter on page 23.

To execute a advanced search

ⓘ **NOTE:** The advanced search is available at places where requests are listed. Examples of these places would be the **Requests** tab in an employee's detailed view under the menu **My Responsibilities | People** or **Auditing | Employee details**, .

1. Click **Advanced search** in the detailed content view.

   The following options are available:

2. Click **Search** or press **Enter** to run the search.

Table 14: Setting options for advanced search

Category	Setting	Description	Occurs
Display requests	Requests submitted by you for yourself / Requests submitted by the selected employee for himself	If the option is set.	• Request History • Auditing - <selected employee> - tab **Requests**
	Requests submitted by you for others / Requests submitted by the selected employee for others	If the option is set.	
	Requests submitted by others for you / Requests submitted by others for the selected employee	If the option is set.	
	Requests submitted by other users Submitted requests in the selected employee's organization	If the option is set.	
Filter by request number	Text box for number to search for.	Searches for number entered.	• Request History • Approval History • Auditing - <selected employee> - tab **Requests** • Auditing - Requests • Auditing - <selected employee> - tab **Approvals** - tab **Approvals** • Auditing - Approvals

Category	Setting	Description	Occurs
Request state	Pending	Searches for all pending requests.	• Request History
	Approved	Searches for all approved requests.	• Approval History
			• Auditing - <selected employee> - tab **Requests**
	Canceled or denied or dismissed	Searches for canceled or denied or dismissed requests.	• Auditing - Requests
			• Auditing - <selected employee> - tab **Approvals** - tab **Approvals**
			• Auditing - Approvals
Delegations	Valid from	Specifies the start of the time period.	• Delegation history
	Valid until	Specifies the end of the time period.	
	Delegator	Selection of delegator.	
	Delegation recipient	Selection of the delegation recipient.	
	Show never assigned delegations	If the option is set.	

Sorting

To sort a table

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

    You will see an ⯆ icon to the right of the column name.

2. Click again in column header to sort in ascending or descending alphabetical order.

    This sorts the column as required.

3. Click again in the column header to sort in the opposite order.

    This resorts the column.

To sort a table by several columns

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

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

Table 15: Multiple column Sorting

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

Working with Bookmarks

You sometimes have the option to set bookmarks in views in the Web Portal. Bookmarks are displayed on the start page and in the Web Portal header. Bookmarks can be deleted again where they were set or on the start page. Bookmarks have the advantage that you can use them to navigate straight to a particular part in the Web Portal when you log in again.

To set a bookmark

- Select an entry from the menu **My Responsibilities** in the **System Entitlements** view, for example, and create a bookmark by clicking 🔖.

  The link **Bookmark this page** changes to **Delete favorite**

To use a bookmark

- Perform one of the following tasks.

    a. Click the bookmark on the start page.

    b. Click 🔖 in the header and select the bookmark you want to retrieve.

  This navigates to the page with the data you have bookmarked.

To delete a bookmark

ⓘ | **NOTE:** You must select the bookmark in order to delete it.

- Delete the bookmark by clicking 🔖.

  The **Delete favorite** link changes back to **Bookmark this page**. The bookmark is no longer displayed on the start page or in the header.

Using a Filter

The filter function is represented by ▼ and provides various types of filters. It is available in all table columns.

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

To use filter on a column

- Open a menu, which shows a view with tables.
- Click ▼ in the selected column.

To apply filter criteria to text

1. Enter one or more terms in **Filtering on...** in the dialog box.

2. Select one of the following criteria from the menu.

   Table 16: Other criteria for applying filters to text boxes

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

To apply filter criteria to numerics

1. Enter a value in the numeric field.

   ⓘ | **NOTE:** You can adjust the value using the arrows next to the value.

2. Select one of the following criteria from the numeric filter's menu.

   Table 17: Other selection criteria for using numeric filters

Filter	Description
At least	Only results with a value the same or higher than the given value are shown.
Lower than	Only results with a lower value than the given value are shown.
Between	Only results with a value the between the given values are shown.

To apply an object filter

1. Select the **Filter by object** tab.

   The results are shown, by default, in a hierarchical structure.

   - Open the hierarchy by clicking on ▶. Repeat this step if necessary to display more objects.
   - Click ▦ to change to list view.
   - Click ⬚ to return to the hierarchical view.

2. Click ⊗ to mark the required object.

   The selected object is labeled with ⊘ and listed under **Selected** in the detailed content view.

   ⓘ | **NOTE:** To deselect an objects, click on the object in the detailed content view.

3. Click **Filter on**.

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

To apply filter criteria to the calendar function

1. Select one of the following criteria on the menu next to the text box.

   Table 18: Other criteria for applying filters to the calendar function

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

2. Perform one of the following tasks.

   a. Click the calendar icon and select a date.

   b. Enter the date in the text box.

3. Click **Filter on**.

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

To delete a filter

Perform one of the following tasks.

1. Click ✖ in the filtered column.

2. Click ✖ in the row above the entire table.

To group by column

ⓘ | NOTE: The button **Group by column** is only available in certain columns in the dialog box **Filter on...**.

1. Select the filter for the column you want and click **Group by column** in the dialog box.

2. Open the group with ＞ .

   This displays all the entries in the group.

To revert a grouped view

- Delete the filter.

  This dissolves the group.

To include other columns in the table

1. Click **Additional columns** above the table.

   This open the selection dialog **Additional columns** displaying a list of additional columns.

2. Configure your settings.

This selects the column. Multi-select is possible.

3. Click **Apply**.

   Now you can see the column in the table and use it.

To save the current view

ⓘ **NOTE:** If neither a filter nor a default value was set in the dialog box **Filter on**, you cannot select or edit view settings in the context menu under **View settings**.

1. Apply the filter.

   Once a filter has been applied, it is displayed in a gray bar above the column.

2. Click **View settings** and select **Save current view** from context menu.

   This opens the dialog box **Save current view**.

3. Enter a name for the filter in the text box and click **Save**.

   You can now select the new filter in the **View settings** menu.

To remove a saved view

ⓘ **NOTE:** A gray bar with the filter setting appears above the table if a saved view is enabled. You can also view the filter setting in the **Filter on ...** dialog box.

1. Click **View Settings** and select **Edit list** from the menu.

   This opens the dialog box **Edit view settings**.

2. Click 🗑 after the view setting you want to delete.

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

Working with Custom Filter Conditions

At certain points you can define custom filter conditions. The filter conditions are formulated like a condition (WHERE clause) for a database query.

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

The wizard is available in different places in the Web Portal, for example, in the **People** view.

To open the filter wizard

- Select the entry **Open filter wizard** in the **View Settings** menu.

To create and apply a filter with the wizard

1. Open the filter wizard from the table you want to create the filter for.

2. Select the column in the filter wizard.

   a. Click the link **At least one entry exists** and specify whether the column should reference or be referenced from other tables.

      The following tabs are available.

Table 19: Tabs in the Filter Wizard

Tab	Description
Value comparison	Compares the values of the selected columns.
	These columns are part of the table you want to apply the custom filter to.
	The advantage of using the where clause wizard is that you can select all the table's columns as opposed to the filter function, which only provides a default selection of columns.
References to other objects	Creates a n:1 relation.
	Select the desired table B on this tab. Several data records from table A can be assigned to one data record in table B. A data record in table A cannot be assigned more than one data record from table B.
References for assignment tables	Each data record in table A can be assigned to several data records from table B and vice versa. These relations are realized through a third Table for realizing assignment tables Assignment table only contains the foreign keys of the other tables A and B.
References of other objects	Creates a 1:n relation.
	Select the desired table B. Several data records from table B can be assigned to one data record in table A. A data record in table B cannot be assigned more than one data record from table A.

b. Select the column you want on the tab in the **Filter wizard** view.

This inserts a control for the first condition.

Figure 1: Filter Wizard with Examples of Conditions
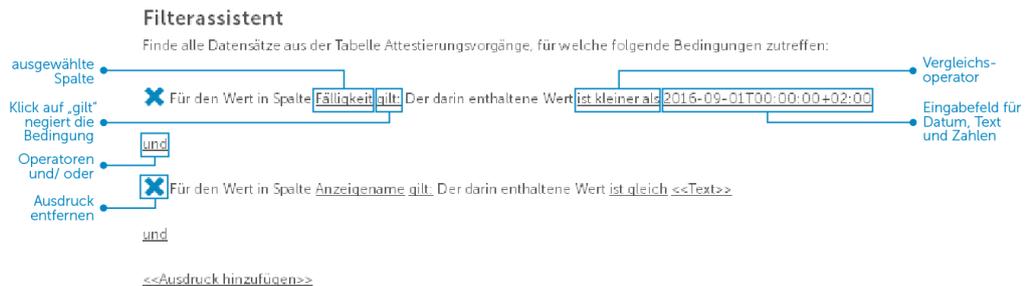
3. Enter the condition and configure the following settings:

a. Enter the comparison value.

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

b. Change the comparison operator.

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

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

Table 20: Comparison Operators

Value type	Operator	Description
Text	is equal to	Searches for the same text string.
	precedes the word in the alphabet	Searches for all results that precede the given text alphabetically.
	follows the word in the alphabet	Searches for all results that follow the given text alphabetically.
	not equal	Searches for all results that do not correspond to the text.
	is contained in	Searches for all results that contain the text.
	contains	Searches for all results that contain the text.
	starts with	Search for all results that begin with the given text.
	ends with	Searches for all results that end with the given text.
	is equal or precedes the word in the alphabet	Searches for all results that either contain the given text or precede it alphabetically.
	is equal or follows the word in the alphabet	Searches for all results that either contain the given text or follow it alphabetically.
Numeric	is less than	Searches for all results that are less that given number.
	is greater than	Searches for all results that are greater than the given number.
	equals	Searches for all results that are equal to the given value.
	is less or equal	Searches for all results that are less than or the equal to the given number.
	is greater or equal	Searches for all results that are greater or equal to the given number.
	not equal	Searches for all results that do not match the given number.

c. Change the Boolean value if the option is available.

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

d. Negate the condition by clicking **the following applies**.

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

    e. Use the operators `and` or `or` if there is more than one condition.

    ⓘ | **NOTE** Remove a control by clicking ✖.

4. Insert another expression by clicking **<<Add expression>>** and repeat this step if required.

5. Perform one of the following tasks.

    a. Apply the filter by clicking **Apply**.

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

    b. Close the wizard by clicking on **Close**.

To expand or collapse controls.

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

1. Perform one of the following tasks.

    a. Click **Collapse all** in the **Filter wizard** after you have a applied a filter with multiple conditions and controls.

    b. Click **Expand all** if the controls are collapsed.

To view difference between data records

1. Open the filter wizard.

2. Click **View comparisons**.

   This opens the following tabs.

Table 21: Description

Tab	Description
New matches	Displays new data records, which are added to the originally displayed data records after filtering.
Unchanged matches	Shows all the data records that are affected by the filter and included in the results.
Removed matches	Show all data records that no longer fulfill the filter criteria after the filter has been applied.

3. Select the desired tab and view the results.

    ⓘ | **TIP:** A maximum of 200 data records are displayed. To limit the results, enter a search term in the text box.

4. Enter a term in the search box to limit the results if required.

To display technical names of database columns

1. Open the filter wizard.

2. Click on **Show technical name**.

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

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

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

ⓘ **NOTE:** To open the expert view, you must own the role of administrator, auditor or Compliance § Security Officer.

1. Click **Export view**.

   If you have already created a filter, the filter condition is shown in the SQL editor as an SQL expression.

2. Perform one of the following tasks.

   a. Edit the SQL expression.

   b. Enter an SQL expression.

3. Perform one of the following tasks.

   a. Apply the filter by clicking **Apply**.

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

   b. Close the wizard by clicking on **lose**.

Exporting a View

The current view can be saved in PDF or CSV format and used as a report. This function is available at different points in your web application. For more information, see Viewing Reports in the Web Portal on page 118.

ⓘ **NOTE:** Only a maximum of 100 000 data sets can be exported. If there are more data set, only the first 100 000 are exported.

To export a view

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

1. Click **Export this view** in the view above.

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

2. Enable the following options if required:

   - All pages
   - Remove header

3. Perform one of the following tasks.

   a. Select either **Export as PDF**.

   b. Select the option **Export as CSV**.

4. Click **Export...**.

   The corresponding report is generated and displayed according to your settings or you are asked whether you want to save o open the report.

Switching Between the Mobile and Desktop Views

The Web Portal is designed for use with desktops computers and mobile devices. You have the option to swap between these two user interfaces in your web application. For more information, see Getting Started with the One Identity Manager Web Portal on page 8.

To change to the mobile view

1. Click 🛈 in the header.

   This opens a menu with other menu items.

2. Select **Switch to mobile view**.

   This changes to the mobile view.

   🛈 | **NOTE:** If your mobile device does not have a touchscreen, you can use your mouse cursor to click on the desire point instead of swiping or tapping the display.

Table 22: Handling Options for Mobiles

Action	Handling
Open the navigation menu	Perform one of the following tasks. • Tap ❯ on the screen in the breadcrumb navigation. • Touch the screen and drag from right to left.
Close the navigation menu	Perform one of the following tasks. • Tap ❯ on the screen again. • Touch the screen and drag from right to left.
Switch to the desktop view	1. Tap on 🛈 in the header. 2. Select **Switch to desktop view** by tapping on the menu.

Detailed information about this topic

- Hyper Views and Mobile Devices on page 31
- Heatmaps and Statistics for Mobile Devices on page 33

Hyper Views and Mobile Devices

You have many more ways to handle your web application in the mobile view than in the familiar desktop view. In this chapter, you will be shown the names and descriptions of handling options for Hyper Views. Other common handling options for mobile devices are described in a separate chapter. For more information, see Switching Between the Mobile and Desktop Views on page 31.

Table 23: Handling Options for Mobiles

Action	Handling
Move a Hyper View or shape	• Touch the Hyper View or shape on the screen and drag it to the desired position.
Zoom in or out on a Hyper View	ⓘ **TIP:** If your mobile device does not have a touch screen, move the Hyper View by pressing and holding the SHIFT key and left mouse key (this is not support by all browsers) over the screen. There are two circle elements visible on the screen that move apart (zoom in) or together (zoom out) when you move the mouse.
	Perform one of the following tasks.
	a. Touch the screen at two points at the same time and drag the points away from each other. The entire Hyper View is zoomed in.
	b. Touch the screen at two points at the same time and drag the points together. The entire Hyper View is zoomed out. - OR -
	a. Double-tap anywhere on the screen.
	b. Double-tap again anywhere on the screen.
Expand or collapse a shape	ⓘ **NOTE:** The main shape or central shape in the Hyper View is always expanded and cannot be collapsed. All other shapes are collapsed when the Hyper View is loaded.
	Shapes that have a button at the top right can be expanded. You can view more detailed information in the expanded view.
	You can click on or tap some elements in the shape to show more details. Use the breadcrumb navigation or the **Back** button in your browser to return to your starting point.
	1. Tap on the shape. The shape is expanded and you can see the entire contents.
	2. Tap in the shape's header. This collapses the shape.
Zoom in or out on a shape	1. Touch the shape on the screen and hold. The shape zooms in by a fixed amount.
	2. Release your hold. The shape returns to its original size.
Display a shape of a Hyper View on the screen	• Tap **Overview** on the screen. The Hyper View changes its size so that as many of the shapes as possible are visible on the screen.

Action	Handling
Display a hyper view in its original size	• Tap **Centered** on the screen. The Hyper View is displayed in its original size again.
Open or close all shapes in a Hyper View	1. Tap **Expand** on the screen. All shapes in the Hyper View are expanded at the same time. Now **Collapse** is displayed on the screen instead of **Expand**. 2. Tap **Collapse**. All the Hyper View shapes are collapsed at the same time.

Detailed information about this topic

Heatmaps and Statistics for Mobile Devices

Not only does handling of Hyper Views vary between desktop and mobile views but also the handling of heatmaps and statistics. The following handling options apply to heatmaps and statistics.

Table 24: Handling Options for Heatmaps and Statistics

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

Detailed information about this topic

Working with the Web Portal

The standard Web Portal is a tool that you can use to manage the following resources in your organization. The Web Portal is customized to suit your needs. Its functionality is dependent on your roles and ownerships.

Detailed information about this topic

Making and Managing Requests

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

- Group or system entitlements (for example, Active Directory®, SharePoint®, IBM® Notes®, SAP® R/3® and so on).
- Membership in roles (for example, business roles, departments, application roles and so on).
- Access to a file system or SharePoint® resource.
- Every other resource in your area.

When you make a request, it triggers a workflow. Although the given workflow may be different, what generally applies is:

- Your request is forwarded to an approver.
- An approved request is forwarded to the employee responsible for processing.
- You are notified whether your request is granted or denied.

You can run various actions in the **Request** menu. For example, you can view the status of your request, or may be able to make requests on behalf other employees. You can navigate to request from the start page or through the menu **My Actions** and **Request**.

Detailed information about this topic

Making a Request

The request process is triggered when you request a product. You can make a request for any suitable products. Whether you are authorized to request a product depends on your role and your permissions. Managers or other authorized users can make request for other employees in their name.

- Requesting through the Search Function
- Requesting through a Service Category
- Requesting Products with Dependent Products
- Requesting from a Template
- Requesting through a Reference User
- Making Requests for Other Recipient
- Renewing Requests
- Resubmitting a Request
- Creating and Editing Request Templates
- Requesting a Starling 2FA Token
- Requesting Products requiring Multi-Factor Authentication
- Special Requests
- Other Request Options - Request Group

ⓘ | **NOTE:** Requestable products have been configured and made available by an administrator in the Manager. Products are configured by assigning request properties and determining associated products and/or optional products. For more detailed information about configuring the IT Shop, see the Dell One Identity Manager IT Shop Administration Guide. The IT Shop is part of the Web Portal which you can use for making requests. Use the Manager's administrators to configure the IT Shop and for preparing products for requesting in the IT Shop.

Requesting through the Search Function

If you do not know the exact name of the service item for your request, you can use a keyword search to help you. You have the search function in the **Request** menu or the Web Portal's global search available to do this. In the menu **Request**, you also have the possibility to search in all service categories or only one selected service category. Prerequisite for this kind of search is that keywords have been added by their product owners. For more information, see Adding Tags for Service Items on page 84. For more detailed information about tags, see the Dell One Identity Manager IT Shop Administration Guide.

To search for service items in all service categories with the help of keywords

1. Click **Service Catalog | Request**.

2. Enter a keyword or part of one in the text box **Find a service item** in the **Request** view and click 🔍.

   This displays a list of the service items found. For more information, see Requesting through a Service Category on page 36.

ⓘ **TIP:** If you use the Web Portal global search to find the service item you want, you must enter more than two letters into the search field to get a result.

To search for a service item within a selected service category with the help of keywords

1. Click **Service Catalog | Request**.

2. Select a service category in **Request** view.

3. Enter a keyword or part of one in the text box in the **Request** view and click 🔍.

    This displays an overview of the resulting service item within the selected service category. For more information, see Requesting through a Service Category on page 36.

Requesting through a Service Category

You can execute requests through service categories in **Service catalog | Request**. After you have selected a service category, you may be presented with other groups and products in this service category.

You can search for products without preselecting a service category. For more information, see How to Search on page 19. The filter function provides you with another way to find a product you want by filtering the list of products. For more information, see Using a Filter on page 23.

There are products in the list that are marked with an icon. The meaning of these icons are explained with relevance to the product, in the table below.

Table 25: Request Status

Icon	Status
✅	The product was requested and has already been assigned. You cannot make another request at the moment.
❌	The product was already requested or it is not currently available. It cannot be requested at the moment.
↳	A pending request already exists for this product. You cannot repeat the request at the moment.
ⓘ	The product was already assigned to the user. The product assignments can be inherited, for example. It is not possible to make another request for this product. If the request is repeated, the status changes to **This product has already been requested**.

To request products through a service category

1. Open the menu **Service catalog | Request** and click on the service category you want in the main view.

    In the **Request** view, the selected service category is shown as a highlighted link and the products that are in it are listed. Click ⬅, if you want the change the selected service category or return to the start page of the **Request**. Grouped service categories are displayed with ▼ and offer other selection options. For example, a service category with grouping is the service category **Active Director Groups**.

2. Enable the option **Include child categories** to display main and sub categories in the same list.

3. Perform one of the following tasks.

    a. Select the group you want from on of the grouped service categories.

a. Enter the product in the search box and click 🔍.

This displays the product.

4. Perform one of the following tasks.

a. Mark the product and click **Request**.

b. Enable the product's check box.

5. Enter other data about the product in the dialog window and confirm with **OK**.

6. Click **Submit request now**.

7. The **My Shopping Cart** view is displayed.

8. Perform one of the following tasks.

a. Edit your shopping cart.

For more information, see Editing Requests within your Shopping Cart on page 45.

b. Click **Check & submit shopping cart**.

This displays a message about the request.

Requesting Products with Dependent Products

To request a product with dependent products

Example: Paper and color cartridge are ordered together for the printer. There is a condition that color cartridges may only be requested once a month. You can always request paper. Paper and toner was requested at the beginning of the month. The paper usage is higher than normal and is used up before the end of the month. The paper request cannot wait until next month and must be requested now without cartridges.

1. Open the menu **Service catalog | Request** and select the product you want.

2. Enter any other data about the product in the dialog window and confirm with **OK**.

Your request is listed in the **My Shopping Cart** view.

ⓘ | **NOTE:** If the dependent product has not been not requested as yet, it is automatically requested as well.

3. Perform one of the following tasks.

a. Open dependent items and click ▶.

Another item appears below the request.

b. Mark the request in the **My Shopping Cart** view.

ⓘ | **NOTE:** In the detailed content view you can enter a reason for these items, edit and enable the **Valid from** and **Valid until** dates. Other actions are not possible.

4. Click **Check and submit shopping cart**.

Requesting from a Template

You can create requests from your own templates or system templates. This helps simplify proper provisioning for a particular job or function. For example, a template may contain all the products a new employee 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. For more information, see Creating and Editing Request Templates on page 40.

To make a request using a template

1. Open the menu **Service Catalog | Request**.

2. Select **Select a request template** from the **Actions** menu.

   This opens the dialog box **Choose a template**.

3. Open the template you want to use by clicking ▶.

   This displays the products in the template.

4. Select the template.

   The selected template is displayed in the **My Shopping Cart** view.

5. Enter a reason and dates, if required, in the detailed content view.

6. Perform one of the following tasks.

   a. Click **Edit shopping cart**.

      This opens a dialog box for the shopping cart. You can enter a comment and other information about your shopping cart. This data applies to all items in the shopping cart.

   b. Click **Check & submit shopping cart**.

      The request is checked and the dialog box **Submit shopping cart** is shown.

   c. Confirm the prompt with **OK**.

   For more information, see Editing Requests within your Shopping Cart on page 45.

Requesting through a Reference User

You can use this option to request products, which have been assigned to the selected (reference user) employee on this date.

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

1. Open the menu **Service Catalog | Request**.

2. Select an authorized user using the **Select reference user** in the **Actions** menu.

   ⓘ | **NOTE:** The list of employees can be extended with more information. Click **Additional columns** and select the information you require from the dialog box.

3. Perform one of the following tasks.

   a. Select a person from the list in the **Select an employee** dialog box.

   b. Select an employee in the **Current** list to deselect him or her.

   This lists requests, memberships and entitlements depending on which requests this employee has made or in which organizational structures a membership exists or similar.

4. Enable the item you want (multi select is possible) and click **Add to shopping cart** or press **ENTER/RETURN**.

   This shows your shopping cart. For more information, see Using your Shopping Cart to Submit your Requests on page 44.

Making Requests for Other Recipient

You can make requests for other employee if you have sufficient permissions. For example, a department head has these permissions. You can only request products from shops where the employee is customer and for whom you are responsible.

You can see what products this recipient already has by clicking the **Check requests for this recipient** link for this recipient.

ⓘ | **NOTE:** You can filter the list of recipients. For more information, see Tips for using the Web Portal on page 18.

If there are people assigned to your area of responsibility, you can also use requests from the cart for another person.

To make a request for another recipient

1. Open the menu **Service Catalog | Request** and click **Change** next to **Recipients**.

    ⓘ | **NOTE:** The list of employees can be extended with more information. Click **Additional columns** and select the information you require from the dialog box.

2. Request the product you want for this employee.

Detailed information about this topic

- Requesting through a Service Category on page 36
- Requesting from a Template on page 37

Requests for Subidentities

Requests can be made for subidentities in the same way as for other recipients. 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.

To request a subidentity

ⓘ | **NOTE:** You are logged in with your main identity in the Web Portal.

1. Open the menu **Service catalog | Request** and click **Change** next to **Recipient**.

    ⓘ | **NOTE:** The list of employees can be extended with more information. Click **Additional columns** and select the information you require from the dialog box.

2. Select a subidentity from the list.

3. Request the desired product.

Renewing Requests

Some requests are only valid for a limited period. You can apply for a renewal of this request at any time. Renewals are processed in the same way as a request. Renewals are forwarded to the appropriate approver for approval. The renewal does not come into effect until it has been authorized. If the renewal is denied, the request expires on the given date.

ⓘ | **NOTE:** You are notified 14 days before your limited period request expires. You can renew the request after receiving this message. The requests are automatically canceled once they have expired.

To renew a request

1. Open **Service Catalog | Renew**.

   All requests are displayed with and without time limits. Sort the requests by validity to list the limited requests sequentially.

2. Renew a request in the name of another employee.

   For more information, see Making Requests for Other Recipient on page 39.

3. Enable the request you want to renew and click **Renew**.

4. Edit the renewal date in the dialog box and save the changes.

   The request is moved to your cart. For more information, see Editing Requests within your Shopping Cart on page 45.

Resubmitting a Request

If a request was canceled, aborted or denied, you can resubmit the original request, This can be processed faster than submitting a new request and retains the request history.

To resubmit a request

1. Open the menu **My Action History | Request History**.

2. Select the request you want from the **Request History** view.

   This displays more information in the detailed content view.

3. Click **Submit again**.

4. Enter a reason for resubmitting in the request and click **OK**.

   The request is added to your shopping cart. For more information, see Editing Requests within your Shopping Cart on page 45.

To search in the request history

- Use the extended search.

   For more information, see How to Search on page 19.

Creating and Editing Request Templates

This menu item shows all templates you have created yourself and system-wide templates (created and published by others). By default, products in a template are hidden. You can expand the template you want and view the products and edit them. For more information, see Requesting from a Template on page 37.

Table 26: Templates – Status

Status	Meaning
⚪	This template has not been approved yet. A decision about publishing it still pending.
🟠	The template is marked for public use but was not published yet.
🟢	The template was published.

To create or edit a request template

1. Add your request to the shopping cart.

    For more information, see Tracking your Request on page 49.

2. Open **My Shopping Cart** and select the action **Create template from shopping cart**.

    ① | NOTE: The list of requests and options for handling them is only shown when there are requests
    in the shopping cart.

    In the upper part of **Cart templates** you can see the contents of the shopping cart. Existing request templates are listed in the middle part.

3. Perform one of the following tasks.

    a. Select a request template and click **Select**.

    b. Enter a name for the new template in **Name of the new template**.

4. Click **Create template**.

To delete an item or an entire template

1. Open **Service Catalog | Maintain Templates**.

2. Perform one of the following tasks.

    a. Select your template and click [icon] if you want to delete the entire template.

    b. Click [icon] next to the request template.

        The template is displayed with all the items it contains.

        - Mark the item you want to delete and click [icon] .

3. Confirm the prompt with **OK**.

To share your template with other users

1. Open **Service Catalog | Maintain Templates**.

2. Select your template and click [icon] .

3. Enable the options **Template is available to other employees** and **Template has been approved** in the dialog box.

    ① | NOTE: Enable this option if you do not want to make any more changes to template. After you
    have completed all changes to the template, enable the option **Template has been approved**.

4. click **Save**.

To add more information to a request

1. Open **Service Catalog | Maintain Templates**.

    The view **Cart Templates** is displayed.

    ① | TIP: Click [icon] next to the template to expand the contents and view each item.

2. Select your template and click [icon] .

    This opens the dialog box **Edit template**.

3. Enter the desired information in the text boxes and enable the options.

4. click **Save**.

Requesting a Starling 2FA Token

The Starling Two-Factor Authentication is a multi-factor authentication and is required for requesting certain products in the Web Portal.

To use multi-factor authentication, you must have a Starling 2FA token. You can request this product in the Web Portal. The following data is required to request a Starling 2FA token.

Table 27: Data for Requesting a Starling 2FA Token

Data	Description
Mobile telephone number	Your mobile phone number is mandatory for multi-factor authentication. You can add this to the **Contact** tab under **My Settings** if it is not already there. For more information, see Updating your Contact Information on page 10.
Country	Entering the country where you live is mandatory. You can add this in the same way as your mobile phone number, under **My Settings**.
Default email address	You can also add this in the same way, under **My Settings**.

To request a Starling 2FA token

ⓘ **NOTE:** Each employee can only request one new Starling 2FA token. If your mobile number changes, you must cancel the product and request it again.

1. Open the menu **Service Catalog | Request** and click **Access Lifecycle** in the main view.

2. Mark the product **New Starling 2FA token** and click **Request**.

3. Check the mobile number in the dialog box and the country code and confirm the prompt with **OK**.

4. Check the request in your shopping cart and click **Check & commit shopping cart**.

5. Confirm the prompt with **Yes**.

   The request is forwarded to your manager for approval. Once your manager has granted approval, you will receive a text message on your smartphone with a link to a two-factor authentication app.

6. Install the app on your smartphone.

   a. Open the text message and click on the link.

   b. Load multi-factor authentication on your phone.

   c. Open the app and enter your country code and the mobile phone number.

   d. Confirm the given data and enter your email address.

   e. Reconfirm and select whether to use telephone or text message contact.

      After successful installation, you will receive a registration code.

   Now you can use the app to generate security codes.

Requesting Products requiring Multi-Factor Authentication

Some products in the Web Portal can only be requested using multi-factor authentication. To use multi-factor authentication, you must have a Starling 2FA token. For more information, see .

To request a product requiring multi-factor authentication

ⓘ **NOTE:** To provide multi-factor authentication for a product, certain settings must be enabled on the service item and the attestation policy in the IT Shop.

1. Open the menu **Service Catalog | Request** and select the product.

2. Check the request in your shopping cart and click **Check & commit shopping cart**.

3. Confirm the prompt with **Yes**.

4. Enable the option **I have read and understood the terms of use** in the **Terms of Use** view and click **Accept**.

   It may take some minutes before you are prompted to enter a security code.

5. Follow the instructions in the dialog box.

   a. Click **Send text**.

      - OR -

   b. Click **Phone call**.

      - OR -

   ⓘ **NOTE:** if the Starling 2FA app is already installed on your mobile phone, you can use it to generate a security code.

   c. Enter the security code in the dialog box and click **Next**.

Special Requests

Certain actions trigger a request when executed in the Web Portal and add it to the cart. The following actions cannot be run from the **Request** menu:

- Adding and Deleting Entitlements to Organizations, Business Roles and System Roles on page 80

- Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services on page 81

- Editing Master Data of Business Roles, System Roles and other Services on page 82

Other Request Options - Request Group

ⓘ **NOTE:** This function is only available if the module Active Directory Module or Target System Base Module is installed.

The service category "Active Directory® Groups", represents another special role in the request process using a service category. During the request process, the group requester must enter the data for the group.

To make a request in the service category "Active Directory® Groups"

1. Open the menu **Service Catalog | Request**.

2. Click the service category "Active Directory® Groups".

3. Enable the selected product in the list of displayed Active Directory® groups.

   More information is displayed about the selected product in the detailed content view.

4. Perform one of the following tasks.

   a. Click **Request** if you want to add more products to your cart.

   b. Click **Submit request now**.

5. Enter a group name in the dialog window and click **OK**.

   The information about the group should contain hints about the naming, type of group and target container. The approver adds the group based on this information. You get more information about the product when you click on the product name.

Using your Shopping Cart to Submit your Requests

Your requests are stored in your shopping cart until you are ready to submit them. Each separate request in your shopping cart is added to a total request and given a shopping cart ID number. If your requests should be submitted later, you can save them in a list.

ⓘ | **NOTE:** Rule checking is only available if the Compliance Rules Module is installed. For more detailed information about rule checking, see the Dell One Identity Manager IT Shop Administration Guide.

The action **Check only** checks whether the requester has the permissions required for the request. The request is also checked for compliance violations. After validation, a prompt appears to confirm whether you want to submit the request.

ⓘ | **NOTE:** In certain circumstances, you may cause a compliance violation when you grant approval to a request, which allocates a specific entitlement to a business role. For example, an employee may obtain an unauthorized entitlement through this business role. In these cases, the compliance violation is displayed in the detailed content view of the shopping cart.

One of the following icons is displayed in the **Status** column.

Table 28: Checking Status

Icon	Status
✅	Request can be made.
⚠️	Request violates a rule but can still be made.
	This icon can also indicate that a mandatory product is missing.
❌	Request cannot be made due to missing request permissions.
	Or the product has already been assigned.
Advice	If the request verification is still pending, a advice notice is shown in the main context view.

To view your shopping cart

1. Perform one of the following tasks.

   a. Open **Service Catalog | Shopping Cart**.

   b. Click 🛒 in the header.

2. Perform one of the following tasks.

   a. This displays all the items in the shopping cart list on the **My Shopping Cart** tab.

      The **My Shopping Cart** tab is selected by default when you open the menu **Service catalog | Shopping Cart**.

   b. Select the **Details** tab and open the grouped entries and click ❯.

      This expands grouped entries and displays more detail.

3. Use the options in the **My Shopping Cart** view to choose how to display the contents of your cart.

Detailed information about this topic

- Editing Requests within your Shopping Cart on page 45
- Other Edit Options within your Shopping Cart on page 46
- Saving a Request for Later or Moving a Request to the Shopping Cart on page 47
- How to Send a Request, Specify a Validity Period or Priority on page 47
- Dealing with Unsent Requests on page 49

Editing Requests within your Shopping Cart

The **Service Catalog** menu contains several buttons and options which you can use to edit your requests. The buttons and actions are explained in the following table.

Table 29: Edit Options in the menu "Shopping Cart"

Icon/Button	Action
Text boxes	These text boxes are an aid for adding additional information and editing request properties. This additional data could be, for example, that a request violates a compliance rule under specific conditions. The text boxes are also available in a dialog box after submitting a request. Text boxes are provided at the following places: - In the shopping cart - Save for later - Request template
🗑	Deletes the request - From the shopping cart - From the saved for later list - From the request template
💾	Saves additional information in the request's detailed content view.

Icon/Button	Action
Request for multiple employees	Duplicates requests from the shopping cart for other employees. You will find this action action in the main content view in the **Actions** context menu.For more information, see Making Requests for Other Recipient on page 39.
Save for Later	Moves requests from the shopping cart to the saved list. If the list was empty until now, a new tab **Save for later** is displayed next to the shopping cart. You will find this action action in the main content view in the **Actions** context menu.
🛈	Shows the information in the detailed content view about the request currently marked in the shopping cart.
	In some cases, this icon is available as an action on the product if a request with dependent products cannot be sent.
Check only	Verifies the requests in the shopping cart. You will find this function in the context menu in **My Shopping Cart**. After checking, you are informed whether the request can be carried out.
Create template from shopping cart	Creates a template from the shopping cart for reuse. For another employee, for example.
Delete invalid requests	Removes requests from the shopping cart that either violate a rule or require other entitlements. You will find this function in the context menu in **My Shopping Cart**.
Delete shopping cart	Deletes the entire shopping cart contents with one click. You will find this function in the context menu in **My Shopping Cart**.
Edit shopping cart	To edit the shopping cart. For example, to write a reason for the request.
Check & submit shopping cart	Checks and sends the shopping cart for processing. You can find this button at the bottom of the **My Shopping Cart** view.

If the shopping cart does not contain any products, the following options are available in the **My Shopping Cart** view.

- Click here to find products for your shopping cart.

  This link opens the **Request** menu item. For more information, see Making a Request on page 35.

- View the request history

  This links opens the menu item **Request history**. For more information, see Using Views to Get Information on page 106.

Other Edit Options within your Shopping Cart

To copy a request

1. Open **Service Catalog | Shopping Cart**.

2. Mark the request you want on the **My Shopping Cart** view.

3. Select the employees using the action **Request for multiple employees** in the detailed content view (multi-select is possible).

4. click **Save**.

   The **Request for multiple employees** is closed and the requests for the selected employees are displayed under the requests already listed.

To delete a request from your shopping cart

1. Perform one of the following tasks.

    a. Mark the request you want to delete and click 🗑 in the detailed content view.

    b. Mark a group and then select the action **Delete shopping cart**.

2. Click **Yes** in the dialog box.

To delete all current requests from your cart

1. Select the action **Delete shopping cart** in the **My Cart** view.

2. Click **Yes** in the dialog box.

Saving a Request for Later or Moving a Request to the Shopping Cart

To save a request for later processing

1. Mark the request you want to save in your shopping cart.

2. Select **Save for later** from the **Actions** menu in the detailed content view.

To place a request in the shopping cart

ⓘ NOTE: The saved for later list is displayed as a tab in the **My Shopping Cart** view, assuming a request has already been saved for later.

1. Mark the request you want and select **Add to shopping cart** from the **main Actions** menu in the detailed content view.

    This moves the request into your shopping cart.

2. Open **Service Catalog | Shopping Cart**.

3. Perform one of the following tasks.

    a. Mark the request you just moved and click **Check & submit shopping cart**.

    b. Mark the request you just moved and click **Edit shopping cart information**.

    c. Run another action.

    For more information, see Editing Requests within your Shopping Cart on page 45.

How to Send a Request, Specify a Validity Period or Priority

To submit your requests

1. Open the menu **Service Catalog | Shopping Cart**.

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

    ⓘ NOTE: If this combination of requests is one you might make again, you can create a template. For more information, see Creating and Editing Request Templates on page 40.

3. Mark the request you want and enter more data in the detailed content view.

> ⓘ **NOTE:** The request must have been checked and status set to **OK**.

4. If you want to enter an additional comment about the shopping cart, click **Edit shopping cart information**.

5. Enter a comment about the shopping cart and click **Save**.

> ⓘ **NOTE:** you can test the request for a rule violation by selecting **Check only** in the Actions menu. If a rule violation is found, the request is still being processed and requires further approval from managers.

6. Click **Check and submit shopping cart**.

7. Confirm the prompt with **Yes**.

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

The information **The request was successfully submitted** appears in **My Shopping Cart**.

To specify the validity period for a product request

1. Open the menu **Service Catalog | Shopping Cart**.

2. If you want to edit several requests at the same time, click **Edit shopping cart information**.

   This opens a dialog box for the shopping cart.

3. Enter values to fix the validity period of the requests in **Valid from** and **Valid until**.

> ⓘ **NOTE:** If a there is already a date in **Valid from**, the validity period is determined as from this date and not from the approval date. The same applies for the **Valid until** date. An additional note is displayed in the detailed content view. If the request approval validity period has expired, an error message is displayed and the request is aborted.

4. Save the changes.

To specify the priority of requests

> ⓘ **NOTE:** The **Priority** menu is enabled by default and can be applied. You can disable the **Priority** menu using a configuration parameter in the Web Designer. For more detailed information about enabling configuration parameters, see the Dell One Identity Manager Web Designer Object Model Documentation.

1. Run the first two steps as described in the step-by-step **To specify the request validity period**.

2. Enable the option **Apply to all** in the shopping cart dialog box and select an entry in the menu.

   The following are available.

   Table 30: Priority lists

Priority
Default

Priority
Low
Medium
High

3. Save the changes.

Dealing with Unsent Requests

If your request could not be sent when you executed **Check & summit shopping cart**, you can examine the reason for the failure in your shopping cart. The reasons are marked with the icon you know already, in the **Status** column. For more information, see Using your Shopping Cart to Submit your Requests on page 44.

To view the reason for a failed request

1. Open the menu **Service Catalog | Shopping Cart** and click **Check & submit shopping cart**.

2. Confirm the prompt **Request cannot be submitted** with **OK**.

   Icons are displayed for the products in your shopping cart in the column **Status**, which already indicate which product in your request is causing the problem.

3. Mark the product with the ⚠️ icon and the note **Missing required product** in your shopping cart.

   Required products are listed int he detailed content view. Required products are dependent products. The action to run or information about how to proceed with each item is displayed respectively. For example, if a required product has already been requested and it can only be requested once, it is not possible to request it again. If the missing required product is still in the request, the action ℹ️ is provided.

4. Click ℹ️ in the detailed content view to view information about where the product is.

   This information is displayed in a dialog box. You can see exactly where your request currently is and whot he approver is on the **Workflow** tab.

Tracking your Request

In the request history, you can see every request you have submitted for yourself or for others. Use the filter function or advanced search to limit the number of requests displayed. For more information, see Tips for using the Web Portal on page 18.

The following compliance states are shown in the request history.

Table 31: Compliance Status in the Request History

Icon	Description
✅	Request does not generate rule violations.
🚫	Request generates rule violations.

The request status of the selected request is displayed, amongst other things, in the detailed content view. The following views may be shown.

Table 32: Request Status in Main View

Status		Description
⬍	Pending/requested	Request is being processed.
✓	Assigned	The request has been assigned.
✕	Denied	The request was denied. The reason for denial is a policy or rule violation or the manager did not check the request, whether the request has a limited period.
✕	Unsubscribed	The request subscription is canceled. For more information, see Canceling Requests on page 50.
✕	Aborted	The request is terminated or the system could not execute the request. This occurs if no one was responsible for checking the request or if the validity period expired. The request history is displayed with the reason for aborting.
✓	Renewal	The request was renewed. For more information about the selected request is shown on the **Information** tab. Information is for example, who submitted the renewal and when.

In the detailed content view, you can view more information about the requests on the **Information**, **Workflow** and **Compliance** tabs.

To view the current status of your request

1. Open the menu **My Actions | Request History** and mark the required request.

2. Select a tab in the detailed content view to view more detailed information.

To withdraw request from the request history

ⓘ | **NOTE:** You can only abort requests with the status Request or Pending.

1. Open the menu **My Actions | Request History** and mark a request with the status "Request" or "Pending".

2. Click **Withdraw request**.

   This opens the dialog box **Cancel request**.

3. Enter a reason for canceling the request in the **Cancel request** dialog and confirm with **OK**.

   The request remains in the request history. The status changes from "Assigned" to "Aborted". The button **Submit again** appears.

ⓘ | **NOTE:** You can resubmit unsubscribed, aborted or denied requests with **Submit again**. Otherwise, the button is not displayed in the detailed content view.

Canceling Requests

You cannot only cancel (or withdraw) requests, you can also unsubscribe them. The difference being that you can only cancel a request within the request process. This means, the request must have the status "Request" or "Pending". You can cancel requests in the request history. For more information, see Tracking your Request on page 49.

Use **Unsubscribe** in the service catalog to unsubscribe a request. These requests must have the status "assigned". Requests with the status "Assigned" are listed in the request history but cannot be subscribed there.

You can unsubscribe products for other employee if you are responsible for them and if you, as approver, granted approval for this product.

> ⓘ **NOTE:** Unsubscribed resources, entitlements and applications are no longer available the next time you log on to the system.

To unsubscribe products

1. Open the menu **Service Catalog | Unsubscribe**.

   All products currently assigned to you are listed.

2. Enable the check box next to the request you want to unsubscribe and click **Request cancellation**.

   This displays the **Unsubscribe** dialog box.

   > ⓘ **NOTE:** Use the **Request** action to display additional products associated with this request.

3. Enter a reason for unsubscribing in the **Unsubscribe** dialog box and click **Save**.

   The unsubscribe request is added to your cart. There you can delete it or save it for later.

To unsubscribe a request on a specific date and time

1. Open the menu **Service Catalog | Unsubscribe**.

   This lists all the requests that have been assigned to you.

2. Enable the check box next to the request you want to unsubscribe and click **Request cancellation**.

   This displays the **Unsubscribe** dialog box.

3. Enable the control box **Unsubscribe on** and specify a desired date and time.

4. Enter a reason for unsubscribing and click **Save**.

   The edited request is then listed with the new validity period under the **Unsubscribe** and **Renew** menus. More details are displayed in the detailed content view on the **Workflow** tab.

Processing Pending Requests

Many requests go through a manual approval process, in order to ensure the correct assignment of products. You may be required to approve or deny requests, for example if you are a manager. You can make inquiries in cases where you need more information to make a decision, add more approvers, or reroute the request.

You can see more detailed information about a pending request in the detailed content view.

Table 33: Detailed content view of a pending request

Tab	Description
Information	Displays all information about a request. The information displayed varies and is dependent on the service category from which the request was triggered. The following data can be displayed. • Product • Recipient • Requester • Processing status • Priority • Request date • Valid from • Valid until • Renewed until • Reason You do not have to fill all the properties. None of the information can be edited or clicked on apart from the product, which opens a Hyper View when you click on it.
Workflow	Displays the life cycle chronologically as from the time of request.
Compliance	Displays any rule violations for this request.

ⓘ **NOTE:** Pending requests that have not been granted approval (whether from an approver or automatically is irrelevant) are displayed with a reason in the **Pending requests** view. Reasons are only displayed if approval has been denied, to provide the next approver with an overview as an aid to reaching the next decision. If you want to see the entire approval workflow for this request, select the **Workflow** tab in the detailed content view of the selected request.

Detailed information about this topic

Granting, Denying or Canceling Single Requests

If you are a designated approver for a particular product, when an employee makes a request, it appears on both your home page, and your **My Actions | Pending Requests** menu. You can grant, deny or cancel the request. If you approve a request, the product is available to the employee. You can sort, filter and search on the view. For more information, see Tips for using the Web Portal on page 18.

ⓘ **NOTE:** You can select a predefined text for all undecided approvals in the **Standard reason** text box or using the **Assign** link. Standard reasons are displayed in the approval history and in the case details. For more detailed information about default reasons, see the Dell One Identity Manager IT Shop Administration Guide.

Once you have made an approval decision, the request disappears from your list of pending requests.

To make approval decision about a pending request

1. Open **My Actions | Pending Requests** and mark the request you want in the list of pending requests.

2. Perform one of the following tasks.

    a. Approve the request by clicking on ☑ and click **Next**.

    b. Click on ☒ to deny the request and click **Next**.

    ⓘ **NOTE:** In **Approvals**, you can enter a reason for your approval decision for all open requests or select a standard reason. You can also add the desired information explicitly to the selected request using **Enter reason** or under the displayed date in **Valid thru**.

3. Perform one of the following tasks.

    a. Enter a reason for your approval decision in **Decision** and click **Save decision**.

    b. Select a reason for your approval decision in **Approvals** and click **Save Approvals**.

    The approval decision reason supports the audit trail.

To cancel a request

As approver, you are entitled to withdraw a request on behalf of those responsible.

1. Open **My Actions | Pending Requests** and mark the request you want in the list of pending requests.

2. Click **Withdraw request** in the detailed content view.

3. Enter a reason for withdrawing it in the dialog box and click **OK**.

Detailed information about this topic

Viewing the entire Request and all Approvals

To view a complete request and approve all pending requests

1. Open **My Actions | Pending Requests** and mark the request you want in the list of pending requests.

2. Select **Show entire request** under **more** in the detailed content view.

3. Perform one of the following tasks.

   a. Grant or deny approval for pending requests by clicking on **Approve all** in the **Pending Requests** view.

   b. Mark the request you want in the **Pending Requests** view and click **Add items to this request**.

Detailed information about this topic

-
-

Approvals about Pending Active Directory® Group Requests

To make an approval decision about a new Active Directory® group

1. Open **My Actions | Pending requests** and mark the Active Directory® group request you want to make.

2. Open the dialog window using **Configure the new group** in the detailed content view and enter the additional data for the new group.

   Table 34: Configure the new group

Setting	Description
Name	Unique name of the new Active Directory® group.
Container	Selected container.
Group type	Selected group type.

3. Save the changes.

4. Perform one of the following tasks.

   a. Approve the request by clicking on ☑ and click **Next**.

   b. Click on ☒ to deny the request and click **Next**.

5. Perform one of the following tasks.

   a. Enter a reason for your approval decision in **Decision** and click **Save decision**.

   b. Select a reason for your approval decision in **Approvals** and click **Save Approvals**.

      The approval decision reason supports the audit trail.

   c. Enter the request's expiry date if necessary and click **Save approvals**.

      ① | **NOTE:** The expiry date setting is only available if the request is granted approval.

Detailed information about this topic

- Viewing Approval History on page 59
- Processing Pending Requests on page 51

Approving Assignment of a New Manager

If a manager wishes to assign a new manager for their employee, they must first select a new manager in the employee's master data and select a deadline for the change-over. This triggers a **New manager assignment** request. For more information, see Assigning a New Manager to an Employee on page 93.

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

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

To make an approval decision about a new manager

1. Open **My Actions | Pending Request** and mark the product **New manager assignment** in the list of pending requests.

   ⓘ **NOTE:** If the employee, for whom you will be manager on the given date after approval is granted, has already received requests or entitlements, you can cancel these on first day.

2. Open the list of assigned entitlements using the link **View user's entitlements** and mark the entitlements you want to cancel.

3. Perform one of the following tasks.

   a. Enable the option **Delete on the effective date** and click **Save**.

   b. Enable the option **Cancel on the effective date** and click **Save**.

4. Perform one of the following tasks.

   a. Approve the request by clicking on ☑ and click **Next**.

   b. Click on ☒ to deny the request and click **Next**.

   The marked request is displayed in the **Approvals** view.

5. Perform one of the following tasks.

   a. Enter a reason for your approval decision in **Decision** and click **Save decision**.

   b. Select a reason for your approval decision in **Approvals** and click **Save Approvals**.

   The approval decision reason supports the audit trail.

   c. Enter the request's expiry date if necessary and click **Save approvals**.

   ⓘ **NOTE:** The expiry date setting is only available if the request is granted approval.

Detailed information about this topic

- Viewing Approval History on page 59
- Processing Pending Requests on page 51

Ask for Help, Delete, Revoke Hold-Status

To ask for help

1. Open **My Actions | Pending Requests** and mark the request you want in the list of pending requests.

2. Select **Ask for help** in the **more** menu in the detailed content view.

3. Perform one of the following tasks.

    a. Select an employee from the list in the **Submit an inquiry about this request** dialog box.

    b. Use the extended search.

    c. Use a filter and then mark the item you want in the result list.

4. Enter your query about the request in **Submit an inquiry about this request** and click **Save**.

    A message, saying that the inquiry was sent, is displayed in **Pending Requests**.

To delete an inquiry

1. Select the request that you made the inquiry about and click **Recall last question** in the detailed content view.

2. Enter a reason for recalling the inquiry in **Recall last question** and click **OK**.

To revoke hold status

ⓘ | **NOTE:** Questions asked about a pending request that have been answered, are given hold status in the approval workflow.

1. Mark the request you want to take off hold.

2. Click **Revoke hold status** in the detailed content view.

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

Reroute, Delegate, Add Approver

To reroute an approval

ⓘ | **NOTE:** This action is only available for requested products for which a special approval procedure is required. Employees authorized to make approvals can see this action and reroute an approval. For detailed information about approval procedures for IT Shop requests, see the Dell One Identity Manager IT Shop Administration Guide.

1. Open **My Actions | Pending Requests** and mark the request you want in the list of pending requests.

2. Select **Reroute approval** from the **more** menu in the detailed content view.

3. Select one of the single approval steps in the **Reroute approval** dialog bx and click **Reroute approval**.

4. Enter a reason for rerouting in the text box and click **Reroute approval**.

To delegate an approval

1. Open **My Actions | Pending Requests** and mark the request you want in the list of pending requests.

2. Select **Reroute approval** from the **more** menu in the detailed content view.

This displays the view **Select an employee who should approve instead**.

3. Perform one of the following tasks.

    a. Select an employee from the list in the **Select an employee who should approve instead** dialog box.

    b. Use the extended search.

    c. Use a filter and then mark the item you want in the result list.

    For more information, see Tips for using the Web Portal on page 18.

4. Enter a reason for the delegation in the text box and click **Save**.

    A message, saying that the delegation was sent, is displayed in **Pending Requests**.

    ① | **NOTE:** Delegating an approval means you pass the decision making onto someone else. You, as authorized person, can recall this action in the approval history.

To add more approvers to the request

1. Open **My Actions | Pending Requests** and mark the request you want in the list of pending requests.

2. Select **Add approver** from the **more** menu in the detailed content view.

3. Perform one of the following tasks.

    a. Select in the **Select additional approver** an employee from the list.

    b. Use the extended search.

    c. Use a filter and then mark the item you want in the result list.

    d. Click on the filter icon in **Display** or another column to limit the search for the employee for your inquiry.

    For more information, see Tips for using the Web Portal on page 18.

4. Enter a reason for adding adding another approver in the dialog box and click **Save**.

    A message, saying that the additional approver was entered, is displayed in **Pending Requests**.

    ① | **NOTE:** By adding another approver, you share the approval of this request procedure with the other approver. You, as authorized person, can recall this action in the approval history.

Adding Products to Pending Requests

To add additional products to a request

1. Open the menu **My Actions | Pending Requests** and mark the required request.

2. Select **Show entire request** under **more** in the detailed content view.

3. Click **Add items to this request** in **Request overview** in the detailed content view.

4. Add the products you want to your shopping cart in **Service Catalog | Request** and click **Check and submit shopping cart**.

Confirming Terms of Use for your own Requests

To confirm terms of use for your own requests as the recipient

ⓘ | **NOTE:** If another employee requested a product for you, which requires the terms of use to be confirmed and possibly additional authorization, your approval decision for this request is required. If the requester has confirmed the terms of user for your request, you can view the request under **My Actions | Pending Requests**. Terms of use can only be confirmed if a special approval workflow is explicitly set up for the requested product.

1. Open the menu **My Actions | Pending Requests** and mark the request for which required confirmation of terms of use by the requester.

   In the detailed content view, you can see, amongst other things, information about approval decisions for requests and terms of use on the **Workflow** tab.

2. Perform one of the following tasks.

   a. Approve the request by clicking on ☑ and click **Next**.

   b. Click on ☒ to deny the request and click **Next**.

   The **Approvals** view displays your approvals.

3. Perform one of the following tasks.

   a. Enter a reason for your approval decision in **Decision** and click **Save decision**.

   b. Select a reason for your approval decision in **Approvals** and click **Save Approvals**.

      The approval decision reason supports the audit trail.

   c. Enter the request's expiry date if necessary and click **Save approvals**.

      ⓘ | **NOTE:** The expiry date setting is only available if the request is granted approval.

Editing Pending Requests with the Chief Approval Team

If the are requests pending and the approver responsible is not available for an extended period or has no access to Web Portal, then the fallback approver or member of the chief approval team must make an approval decision. For more detailed information about the chief approval team, see the Dell One Identity Manager IT Shop Administration Guide.

ⓘ | **NOTE:** You only see the menu item **IT Shop escalation approval** if you are a fallback approver or member of the chief approval team.

To make approval decisions about escalated pending requests

1. Open the menu **My Actions | IT Shop escalation**.

2. Use a filter and then mark the item you want in the result list.

3. Perform one of the following tasks.

   a. Approve the request by clicking on ☑ and click **Next**.

   b. Click on ☒ to deny the request and click **Next**.

    c. Click **Approve all** and **Next**.

    d. Click **Deny all** and **Next**.

    ⓘ | **IMPORTANT:** The four-eye rule can be broken like this because chief approval team members can make approval decisions for requests at any time!

4. Perform one of the following tasks.

    a. Enter a reason for your approval decision in **Decision** and click **Save decision**.

    b. Select a reason for your approval decision in **Approvals** and click **Save Approvals**.

        The approval decision reason supports the audit trail.

    c. Enter the request's expiry date if necessary and click **Save approvals**.

        ⓘ | **NOTE:** The expiry setting is only available if the request is granted approval.

To cancel escalated pending requests

1. Open the menu **My Actions | IT Shop escalation**.

2. Use a filter and then mark the item you want in the result list.

3. Click **Withdraw request** in the detailed content view and enter a reason for withdrawing.

Answering Approval Inquiries

ⓘ | **NOTE:** This function is only available if the module Identity Management Base Module or Attestation Module is installed.

You can query requests or attestation cases. The inquiries are displayed in **My Actions | Approval Inquiries**. You can see more information about the inquiry in the detailed content view. There you can see whether you dealing with a request or an attestation case.

For more information, see Processing Pending Requests on page 51.

To answer an approval inquiry

1. Open **My Actions | Approval Inquiries** and mark the inquiry.

2. Click **Answer** and enter an answer.

    The answer is send on saving. Confirmation verification is displayed.

Viewing Approval History

In the approval history, you can view all products you have assigned, denied or canceled, or still being processed (status "Request"). The menu item **Approval History** is the same as **Request History** in its structure and content. For more information, see Tracking your Request on page 49.

To use the advanced search function in the approval history

1. Open the menu **My Action History | Approval History**.

2. Use the extended search.

    For more information, see How to Search on page 19.

To cancel a delegation

1. Open the menu **My Action History | Approval History**.

    This shows all the products you have assigned, denied, canceled or edited.

    ⓘ | **NOTE:** You can only withdraw delegations if the product has the status "Request".

2. Mark the request you want to withdraw and click **Withdraw request** in the detailed content view.

3. Click **Withdraw delegation** in the dialog box.

    ⓘ | **NOTE: Withdraw request** is only shown if approval of this product was transferred to someone else.

4. Enter a reason in the text box in the dialog box and click **Save**.

    For more information, see Granting, Denying or Canceling Single Requests on page 53.

To cancel additional approval

1. Open the menu **My Action History | Approval History**.

    This shows all the products you have assigned, denied, canceled or edited.

    ⓘ | **NOTE:** You can only withdraw additional approvals if the product has the status "Request". Once the approval has been canceled, you are the only approver for this procedure again and can add additional approvers.

2. Mark the request you want to withdraw and click **Withdraw request** in the detailed content view.

    ⓘ | **NOTE:** The button **Withdraw additional approver** is shown if an additional approver was added to this product.

3. Enter a reason for the withdrawal in the text box in the dialog box and click **Save**.

    For more information, see Granting, Denying or Canceling Single Requests on page 53.

Changing Request Priority

You can view pending requests in the **Pending requests** view. The list can be sorted in ascending or descending order. For more information, see Sorting on page 22.

ⓘ | **NOTE:** The **Priority** menu is enabled by default and can be applied. You can disable the **Priority** menu using a configuration parameter in the Web Designer. For more detailed information about enabling configuration parameters, see the Dell One Identity Manager Web Designer Object Model Documentation.

AS an approver of pending requests, you can edit the priority of certain request to influence their position in the sort order. This means, request with high priority are listed at the top if the list is sorted in descending order.

To change a request's priority

1. Open **My Actions | Pending Requests** and mark the request you want in the list of pending requests.

2. Select **Change priority** from the **more** menu in the main content view.

3. Mark the desired priority in **Priority** in the dialog box **Set the priority for this request**.

The following options are available:

Table 35: Priority lists

Priority
Default
Low
Medium
High

4. Click **Apply**.

Editing the Validity Period

As approver, you have the option to extend the validity period of a pending request for an limited period. This is necessary if no approval decision was made within the validity period. Extending the validity period prevents the request from expiring and having to make a new request.

ⓘ **NOTE:** You cannot edit the validity period of requests, which consist of multi-request (not unsubscribable) products.

To configure the validity period for request from multi-request products, you must set the corresponding configuration parameter in the Web Designer. For more detailed information about enabling configuration parameters, see the Dell One Identity Manager Web Designer Object Model Documentation.

To edit a request's validity period

1. Open **My Actions | Pending Requests** and mark the request you want in the list of pending requests.

2. Select **Change validity period** in the **more** menu.

3. Edit **Valid until** in the dialog box **Set the validity period for this request** and click **Apply**.

Request Email Notifications

You can use this menu item to define which events you would like to be notified about through email. This is done by setting check boxes. The possible number of notifications is already configured and you cannot change the setting. The following email notifications are possible:

- Attestation - reject approval
- Attestation - answer
- Attestation - approval required
- Attestation - delegated/additional approval
- Attestation - remind approver
- Attestation - question
- Report subscription - delivery
- Report subscription - delivery to cc

- IT Shop request - canceled

- IT Shop request - aborted

- IT Shop request - expired

- IT Shop request - reject approval

- IT Shop request - answer

- IT Shop request - approval required

- IT Shop request - delegated/additional approval

- IT Shop request - remind approver

- IT Shop request - escalation

- IT Shop request - question

- IT Shop request - not granted approval

- IT Shop request - approval not granted to approval step

- IT Shop request - granted approval

- IT Shop request - approval granted to approval step

- IT Shop request - product expires

- IT Shop request - product change

To enable or disable a mail subscription

1. Click the name of the logged in user in the Web Portal header.

   This opens a menu with other menu items.

2. Select **My Settings**.

3. Select the tab **Mail Subscriptions** in the **My Settings** view.

4. Enable the check box **Mail template** for the mail template you want and click **Save**.

Delegating Roles

ⓘ | NOTE: This function is only available if the module Identity Management Base Module, Business Roles Module or System Roles Module is installed.

The menu item **Delegation** displays all direct and indirect roles. The role classes and associated status are listed along with the roles. You can delegate one or more or all role with your range of responsibility.

Table 36: Delegation Status

Status	Description
Assigned	This status is displayed for the current delegation.
Approved	This status is displayed if you have added a delegation for a later time period.

Detailed information about this topic

-
-
-

Managing Delegations

Your delegations are available under **My delegations | Delegations**. The delegations are managed on two tabs under this menu. You can add new delegations on the **My Roles** tab. Here, all your roles are listed. You can recognize a delegated role by the entry **[count] delegations** in the **Delegated** column on the **My roles** tab.

On the **My delegations** tab you can cancel and delete delegations. All your delegations are listed here. You can cancel and delete approved delegations. These delegations are marked with the **Approved** status. You can only delete delegations, which are not approved. Unapproved delegations have the status **Request** or **Assigned**. The delegation status is displayed in the detailed content view. Individual delegations can also be canceled or deleted on the **My roles** tab.

To add a new delegation

1. Open **My Actions | Delegation** and select a delegate using **Assign**.

2. Enable the check box for the desired role.

   Roles that have already been delegated can delegated again. You can also delegate several roles at the same time, as long as you want to delegate them to the same person.

3. Perform one of the following tasks.

   a. Click **New Delegation**.

   b. Click **All delegations**.

   This opens the dialog box **New delegation**.

4. Configure the following settings in the **New delegation** dialog box and click **Save**.

   Table 37: New Delegation

Setting	Description
Delegate to	Delegation recipient Select an employe using the **Assign** link.
Valid from	Start date and time of the delegation.
Valid until	Expiry date and time of the delegation.
Notify me if the recipient of the delegation makes a decision.	If the option is set, you receive a message in this case.
The recipient can delegate this role	If the option is set, the recipient of the delegation can delegate the role to someone else.

Setting	Description
Role manager	If the option is set, the recipient of the delegation can specify a manager for this role. This option is only displayed when delegating all roles.
Employee manager	If the option is set, the recipient of the delegation can specify a manager for an employee. This option is only displayed when delegating all roles.
Membership	If the option is set, the recipient of the delegation is allowed to edit memberships. This option is only displayed when delegating all roles.
Reason	Text box for entering a reason for delegating.
Priority	Menu for selecting a priority.

The following priorities are available:

- Default
- High
- Medium
- Low

Delegations cannot be changed later. If you should want to make a change, you must withdraw the delegation and set up a new one.

To stop delegation

1. Open **My Actions | Delegation**.

2. Perform one of the following tasks.

   a. Mark the delegation on the **My roles** tab and check the option.

   b. Select the tab **My delegations** and mark the delegation you want to stop.

3. Perform one of the following tasks.

   a. Click on the unapproved delegation in the detailed content view and confirm with **Yes**.

   b. Click **Withdraw request** on the unapproved delegation in the detailed content view and confirm with **Yes**.

Deleting Delegations

Your delegations are displayed on the **My delegations** tab. You can limit the number of delegations displayed by filtering them. You can apply a filter to the column **Type**, for example. Here you can filter the assignment type by the following:

- Employee manager
- Role manager

- Business owner
- Membership

You can delete single or multiple delegations at the same time. You can also delete all delegations in one just step.

To delete one or more delegations

1. Open the menu **My Actions | Delegation** and select the tab **My delegations**.

2. Use a filter and then mark the item you want in the result list.

3. Mark the delegation you want and click on ☑.

4. Repeat this step for each of the delegations you want to delete at the same time.

5. Click **Delete delegation**.

To delete all delegations in the list

1. Open the menu **My Actions | Delegation** and select the **My delegations** tab.

2. Use a filter and then mark the item you want in the result list.

3. Perform one of the following tasks.

   a. Mark all delegations visible in the list and click ☑.

   b. Click **Select all**.

   All delegations visible in the list are marked with ☑.

   ⓘ | NOTE: Click ☑ to deselect the marked delegations. or click ☑ to individually deselect marked delegations.

4. Click **Delete delegation** and confirm the prompt with **Yes**.

   All visible delegations are deleted from the list. If the filter returns more than one page of results, they are displayed on subsequent pages.

To delete all your delegations

1. Open the menu **My Actions | Delegation** and select the **My delegations** tab.

2. Click **Delete all my delegations** and confirm the prompt with **Yes**.

   This deletes the delegations.

Detailed information about this topic

- Managing Delegations
- Using a Filter on page 23

Viewing your Delegation History

In the delegation history, you can view all the delegations you have issued. You can also see the employees you delegated for the task. For more information, see My Action History on page 107.

Adding New Calls

When you add new calls, you report problem cases with different causes. For example, a call can be added for an employee who reports a problem or for products for which conditions of contact were specified. Even a device or workdesk associated with the problematic device, can play a part when adding a call.

To add a new call

1. Open the menu **My Actions | Delegation**.

2. Enter a detailed description of the problem and select the affected product.

3. Set the severity of the problem in **Severity** and select a cost center using the **Assign** link.

4. Select an additional employee using the **Assign** link and click **Save**.

Viewing Call History

In the **Call History** view, you can see all placed calls.

> ⓘ **NOTE:** Use the check boxes at the top of the section to limit the calls shown.

To view a specific call

1. Open the menu **My Action History | Call History** and marked the call in the list.

   More information about the call is displayed in the detailed content view. You can subsequently change **Severity**, **Description** and **Product** entries on the **Master Data** tab.

2. View the staff involved, status and measures taken on the **History** tab.

3. View attachments on the **Attachments** tab.

4. click **Save**.

To delete a file from a call's attachments

1. Open the menu **My Action History | Call History** and marked the call in the list.

2. Select the **Attachments** tab in the detailed content view and click on 🗑 next to the file.

3. Confirm the message with **Yes**.

   This deletes the file from the at**tachmen**ts.

Creating and Editing Reports in the Web Portal

You will find reports in the Web Portal under **My Actions | Reports** or over **My Settings** menu in the header.

In the **Reports** view you can view and edit subscribed reports or create and subscribe to new reports. The view is divided into two parts.

- Available reports and subscriptions

  This section lists all your subscribed reports. You can identity the reports that you have already subscribed to because they are marked with "(1 subscription)" after the report name.

- Owned Reports

  You are responsible for the reports under **Owned Reports** even though you have not subscribed to them. You can view and edit the settings for your reports.

To create a report

1. Open the menu **My Actions | Reports**.

2. Click **Create a new report** in the **Reports** view.

3. Configure the following in the **Create a new report** view.

   Table 38: Setting for a New Report

Setting	Description
Name*	Text box for the report name.
	Enter the report's name.
Report definition	Base table selection.
	Click **Change** to selected a base table from a list.
Columns	Selection of columns from the base table.
	Click **Result columns** to select the columns you want from the base table. This button is only displayed if the base table is selected.
Edit filter	Provides other base tables and columns, which would not normally be available.
	Click **Edit filter** to open the filter wizard.
	For more information, see Working with Custom Filter Conditions on page 26.
Risk index	Display a scale of 0 to 1 for the risk index and two slide rulers.
	Specify a beginning and an end value within the scale.
Owner	Name of the report ownner.
	Click **Change** to select another owner from a list.
Service item	Creating a new service item.
	Click **Create a new service item** to create a new service item.
	You can disable this report definition using the **Disable** option.
Assign to employees	Selecting other employees as report recipients.
	Click **Change** to select an employee to receive the report.

Setting	Description
Assign to departments	Selection of departments to receive the report.
	Click **Assign** to select a department to receive the report.
Assign to Locations	Selection of locations to receive the report.
	Click **Assign** to select locations to receive the report.
Assign to cost centers	Selection of cost centers to receive the report.
	Click **Assign** to select cost centers to receive the report.

4. click **Save**.

Detailed information about this topic

- Viewing and Editing your own Reports on page 68
- Viewing, Subscribing and Editing Reports on page 116

Viewing and Editing your own Reports

You can view your reports and edit the report properties in the **Reports** view.

To view the base table configured for the report

- Mark a report in the **Reports** view and click **Show report**.

  The base tables for this report are shown in the report view.

To view a predefined report

1. Mark a report in the **Report** view and click **View report definition**.

   This displays the tabs **Overview**, **Master data** and **Usage**.

2. Select the tab you want and make any modifications or change the settings.

To edit the report definition

1. Mark a report in the **Report** view and click **View report definition**.

2. Select on the **Master data** tab in the selected report's view.

   You can edit report settings in the **Master data** or add missing data.

To view which roles are contained in a predefined report

1. Mark a report in the **Report** view and click **View report definition**.

2. Select on the **Usage** tab in the selected report's view.

3. Select a role class in the **Role class** menu to see the roles contained in the report.

   For more information, see Usage on page 115.

4. Click **More information** to view employees assigned to the role memberships.

Viewing, Editing and Adding Devices

You can view your devices in the **Devices** view and allocate new devices to yourself. If you have sufficient permissions, you can add new devices or make changes to the device assignments for your staff. For more information, see Managing Devices for Employees on page 94.

To add a new device

1. Open the **My Responsibilities | Devices** menu and click **Add a new device**.

2. Select a device type in **Device type** in the **Devices** view.

   The following device types are available.

   Table 39: Device Types

Device type
Mobile phone
Personal computer
Tablet

3. Assign the model you want in **Device model** and click **Next**.

   This opens the **Devices** view with more input fields. The type of data input required depends on the type of device. Enter the following data.

   Table 40: New Device Settings

Setting	Description
Used by	User for the device.
	The current user is selected by default.
	Use **Change** to select another user from a list. You can only select another user if you own the required permissions or you have your own staff.
Device model	Select a device model.
	You have already entered this in the 3rd step of these step-by-step instructions. Select another device model by clicking **Change**.
Manufacturer	Select a manufacturer.
	Select a manufacturer by clicking **Assign**.
Device ID	Identifier for the device.
	Enter the device's identifier if you know it.
Device status	Select device status.
	Select the device's status by clicking **Assign**.

Setting	Description
Enabling	Activation date.
	Enable the checkbox and enter the activation time and date.
Deactivation	Time and date to deactivate the device.
	Enable the checkbox and enter deactivation time and date.
Asset number *(* only shown if the configuration parameter Hardware\AssetAccounting is set.)*	Asset number input. Enter the asset number if you know it.
Company owned *(* only shown if the configuration parameter Hardware\AssetAccounting is set.)*	Checkbox to define the device as belonging to the company. Enable the checkbox to define the device as company property.
Location description	Location data.
	Enter the location where the device will be used.
Serial number	Serial number.
	Enter the device's serial number, if known.
MAC address	MAC address.
	Enter the device's MAC address.
Storage capacity [GB] / RAM [MB]	Storage capacity / RAM information.
	Enter the device's storage capacity / RAM.
BIOS version	BIOS version.
	Enter the BIOS version if this device is a PC.
Operating system	Name of the operating system.
	Enter the name of the operating system used by the device.
Operating system version	Operation system's version.
	Enter the version number of the operating system currently installed on the device.
Carrier *(* only displayed for mobile phones or tablets)*	Name of the carrier. Enter the name of the carrier to be used with the device.
IMEI *(* only displayed for mobile phones or tablets)*	IMEI number. Enter the IMEI number if this device is a mobile phone.

Setting	Description
ICCID	ICCID number.
(* only displayed for mobile phones or tablets)	Enter the ICCID number (SIM card number) if this device is a mobile phone.
Phone	Telephone number.
(* only displayed for mobile phones)	Enter the telephone number, if this device is a mobile phone.
PC / Server / VM host / VM client	Checkbox for enabling.
(* only displayed for personal computers)	Enable the respective checkbox corresponding to the device.
VM Host	VM host selection.
(* can be edited if the VM client is enabled)	Click **Assign** to select a VM host from the menu.

> ⓘ **NOTE:** Fields marked with * are compulsory.

4. Save the changes.

To edit a managed device

- Mark the device in the **Devices** view and click **Select**.

  On the **Master Data** tab, you can edit the device's settings or add missing ones. For more information, see Table 40 on page 69.

Managing "My Responsibilities"

In the **My Responsibilities** menu you can see tasks and entitlements assigned to you for which you are responsible within your company. You can manage the following responsibilities:

Table 41: Overview of Responsibilities

Responsibility		Objects types
Employees		
Company Structures	Organizations	Cost center
		Department
		Location
	Business roles	
	System roles	
	System entitlements	
	Other services	Resource
	Claim ownership	Active Directory® group

Managing Company Structures

You can use the **Organization** menu to view the departments, cost centers and locations for which you are responsible. Click on the name of the organization to open a with view various tabs. For each tab, you can:

- View a variety of information about the organization (in an overview), its members, entitlements, risk analysis and attestation cases, usage and historical changes to memberships and entitlements. For more information, see Description of Commonly Used Tabs in Views on page 109.

- Add members to the role. For more information, see Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services on page 81.

- Add entitlements to the role. For more information, see Adding and Deleting Entitlements to Organizations, Business Roles and System Roles on page 80.

ⓘ | **NOTE:** As data owner, you can also access pending attestations for which you are the authorized approver, using the **Approver** link on the **Attestation** tab.

Working with Business and System Roles

ⓘ | **NOTE:** This function is only available when the module Business Roles Module or System Roles Module is installed.

Business roles are defined based on the resources needed to perform a particular function. System roles group company resources together in packages, so they can be easy added to employees, and are not dependent on the job the employee performs. You may be able to create new roles. The roles that appear on this list are roles that you are responsible for administering.

ⓘ | **NOTE:** To see roles to which you have been added, view your **Business Roles** overview. To found out which business roles you are responsible for, view **Business Roles** in **My Responsibilities**.

For each business role you own, you may be able to:

- View a variety of information about the business role (in an overview), its members and entitlements, risk assessment and rule violations, attestation cases and usage of various role classes. For more information, see Description of Commonly Used Tabs in Views on page 109.

- Determine if there are any rule violations on the role, by viewing the **Compliance** tab.

- Change the properties of the role. For more information, see Editing Master Data of Business Roles, System Roles and other Services on page 82.

- Add members to the role. For more information, see Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services on page 81.

- Add entitlements to the role. For more information, see Managing "My Responsibilities" on page 71.

To add a new business role

1. Open the menu **My Responsibilities | Business Roles** and click **New business role**.

2. Set the following in the **Create a new business role** view and click **Save**.

   ⓘ | **NOTE:** You must fill in the required fields (marked with an asterisk *). Optional fields can be filled in when you create the role, or later by changing the master data for the role.

Table 42: Properties for new business role

Property	Description
Business role	Text box for naming the application.
Short name	Text box for a name abbreviation.
Internal name	Text box for internal name.
Role classes	Menu for selecting the role class.
Parent business role	Link for selecting the parent business role.
Role type	Menu for selecting the role type.
Role approver	Link for selecting an application role as approver.
Role approver (IT)	Link for selecting an application role as approver (IT).
Managers	Link for selecting an employee as manager. By default, the logged in user is assigned as the manager. The business role is displayed with the manager responsible.
Deputy manager	Link for selecting the deputy manager.
Employees do not inherit	If set, employees are prevented from inheriting.
Description	Text box for entering a reason for the new business role.
Comment	Text box for tips and information.

To add a new system role

1. Open the menu **My Responsibilities | System Roles** and click **New system role**.

2. Set the following in the **Create a new system role** view and click **Save**.

   ⓘ | **NOTE:** You must fill in the required fields (marked with an asterisk *). Optional fields can be filled in when you create the role, or later by changing the master data for the role.

Table 43: Properties for new system role

Setting	Description
System role	Text box for naming the system role.
Display name	Text box for display name.
Internal product names	Text box for internal product name.
System role type	Menu for selecting the system role type.
Service item	Link for selecting a new requestable product.
System role manager	Link for selecting a user as manager. By default, the logged in user is assigned as the manager.

Setting	Description
Comment	Text box for tips and information.
IT Shop	If set, the system role is available through the IT Shop.
	The system role can also be assigned directly to employees and hierarchical roles.
Only for use in IT Shop	If set, the system role is available through the IT Shop.
	The system role may not assigned directly to hierarchical roles.

Comparing an Company Structure's State

You can compare the current state of an company structure with their state in the past in the **History** view. This compares attributes, which have changed within a specified time period. You specify the time period yourself in the date control provided.

As well as comparing a company structure's state, you can also compare an employee's state. For more information, see Comparing an Employee's State on page 94.

The following step-by-step instructions show you how to compare states of an company structure using the example of a **Location** object type.

To compare the state of a company structure

1. Open the menu **My Responsibilities | Organization** and select the **Location** object type you want to compare.

2. Select the **State comparison** tab on the **History** tab.

3. Use 🗓 and ⊘ to set the date and time.

   All the attributes for this employee are displayed in a list. By default, all attributes are selected.

Rolling Back a Business Role to a Historical State

In the **History** view you can roll back the current state of a business role to a state it has had in the past. In the process, you decide yourself which attributes to change. After selecting the business role, all attributes are displayed. These attributes can all be rolled back, with a few exceptions, to a historical state.

In the following table, reasons are listed that prevent roll back to a historical state.

Table 44: Factors Preventing Roll Back

Factor	Description
Attribute was not changed.	Change is not possible without a comparative value.
Membership resulting from delegation.	These memberships are not reset.
Inherited membership	These memberships cannot be deleted.
Membership resulting from a dynamic group.	These memberships cannot be deleted.

To roll back the state of a business role to a historical state

1. Open the menu **My Responsibilities | Business roles** and select the business role you want.

2. Select the **State comparison** tab on the **History** tab.

3. Use 📅 and ✅ to set the date and time.

   All the attributes for this business role are displayed in a list. These include business role properties, memberships, actions, amongst others. By default, all attributes are selected.

   > ⓘ | **NOTE:** If you cannot select an attribute, the check box is not set.

4. Disable the **Roll back** check box and set each attribute you want to roll back, separately.

5. Confirm with **Roll back changes**.

   The selected attributes are displayed in the **Roll back changes** dialog box. You can still change your choice by disabling enabled attributes.

   There are other actions available in the context menu **View settings**, which are listed in the following table.

   Table 45: Entries in the Menu "View Settings"

Menu Item	Description
Reset view	Sets the view back to default after you have, for example, applied a filter.
Save current view	Save the current view to using with filters, for example.
Reload data	Reloads the data.

6. Roll the selected business role attributes back to their historical state with **Roll back**.

Viewing Historical Data about System Roles

You can view historical data for system roles and other accountable company structures on the **History** tab. Although you can view the historical data for system roles, you cannot reset it to a historical state.

The **Overview** shows you all the objects that have been assigned to the system role.

To view historical data for a system role

1. Open the menu **My Responsibilities | System roles** and select the system role you want from the list.

2. Select the **History** tab and select another tab.

   For more information, see History on page 111.

To view system role assignments

1. Open the menu **My Responsibilities | System roles** and select the system role you want from the list.

2. Select the **Overview** tab and click on a shape in the Hyper View.

   The assigned objects are displayed in shapes, which you can click on to obtain more detail.

Working with System Entitlements

ⓘ | **NOTE:** This function is only available when the module Target System Base Module is installed.

System entitlements provide access to the various IT systems in your environment. The following system entitlements are available:

- Active Directory® groups
- LDAP groups
- IBM® Notes® groups
- SAP groups
- SAP structural profiles
- SharePoint® groups
- SharePoint® roles
- Groups of custom target systems

ⓘ | **NOTE:** All system entitlements, which you own, are displayed under this menu.

You can run the following tasks in system entitlements, if you own them.

- View a variety of information about the system entitlement (in a Hyper View), its members, attestation cases and usage of the different role classes. For more information on the tables, see Description of Commonly Used Tabs in Views on page 109.
- Add a new owner role and assign a product owner to an Active Directory® group if you are target system administrator. You can also edit the requestability of a Active Directory® group.
- Change the properties of the entitlement. For more information, see Editing Master Data of Business Roles, System Roles and other Services on page 82.
- Add members to system entitlements. For more information, see Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services on page 81.
- Obtain an overview of all groups that are members of a system entitlement.
- Analyze that state and compare attributes of the base object. You can perform this task in the historical data view. For more information, see History on page 111.

To assign a new product owner to an Active Directory® groups

ⓘ | **NOTE:** This function is only available when the module Active Directory Module is installed.

1. Open the menu **My Responsibilities | System entitlements** and select the Active Directory® group you want.

   ⓘ | **NOTE:** Before you can assign a new product owner, you must add a new owner role for this employee.

2. Select the **Owners** tab and click **Create new owner role**.

3. Enter a name for the new owner role and a reason for creating it.

   ⓘ | **NOTE:** After adding the new owner role, assign a product owner to it.

4. Select a product owner using the **Assign** link and the new owner role using the **Product owners** menu.

ⓘ **NOTE:** If the entry **Without owner in AD** was selected in the **Product owner** dialog box, you cannot select a product owner.

To assign an attestor to a Active Directory® group

1. Open the menu **My Responsibilities | System entitlements** and select the Active Directory® group you want.

   ⓘ **NOTE:** Before you can assign a new attestor, you must add a new application role.

2. Select the **Attestor** tab and click **Create new attestor application role**.

3. Enter a name for the new application role and a reason for creating it.

   ⓘ **NOTE:** After adding the new application role, assign an attestor to it.

4. Select an attestor using the **Assign** link and the new application role using the **Attestor** menu.

To edit requestability settings of system entitlements

1. Open the menu **My Responsibilities | System entitlements** and select the system entitlement you want.

2. Select the **Master Data** tab and enable and set one or more of the IT Shop check boxes and save the changes.

   For more detailed information, see the IT Shop in the Dell One Identity Manager IT Shop Administration Guide.

To add a new group membership

1. Open the menu **My Responsibilities | System entitlements** and select the system entitlement you want.

2. Select the **Subgroups** and click **New subgroup**.

3. Select the group you want using the **Assign** link and click **Save**.

To change the master data of a group managed by Active Roles

ⓘ **NOTE:** This function is only available when the module Active Roles Module is installed.

1. Open the menu **My Responsibilities | System entitlements** and select the system entitlements you want to be managed by an Active Roles.

2. Select the tab **Master data**.

3. To edit the group, check the following boxes:

   - Enable the check box **Only use in IT Shop**.
   - Enable the check box **Approval by group owner**.
   - Enable the check box **Approval by the additional group owner**.

4. Add another owner by clicking **Add account** and click **Save**.

To delete a group membership

1. Open the menu **My Responsibilities | System entitlements** and select the system entitlement you want.

2. Select the tab **Subgroups** and enable the group that you want to delete.

3. Click **Remove selected**.

To assign a device to an Active Directory® group

1. Open the menu **My Responsibilities | System entitlements** and select the system entitlement you want.

2. Select the tab **Active Directory® computer** on the **Memberships** tab.

3. Select the object you want using the **Assign** link and click **Save**.

To view details of an entitlement assignment to a specific member

1. Open the menu **My Responsibilities | System entitlements** and select the system entitlement you want.

2. Select the **Employee** tab on the **Memberships** tab.

3. Mark the employee you want and click ❯ in the detailed content view next to the **Analysis for...**.

    More entries are displayed. Like, the origin of the entitlement and related details.

Managing other Services

In the menu **Other services** you can view resources and applications that you manage. You can execute the following actions for each resource:

- View a resource's overview pages (Hyper View) with all details about memberships, attestation cases and usage. For more information, see Description of Commonly Used Tabs in Views on page 109.

- Change resource properties. For more information, see Editing Master Data of Business Roles, System Roles and other Services on page 82.

- Add new resources and applications.

- Add employees to a resource. For more information, see Editing Master Data of Business Roles, System Roles and other Services on page 82.

To add a new application

1. Open the menu **My Responsibilities | Other Services** and click **New application**.

2. Configure the following settings for the new application and click **Save**.

    Table 46: Settings and data for new applications

Setting	Description
Application name	Text box for the application name.
Version	Text box for the version number.
Language culture	Link for selecting the language.
Service item	Link for selecting a new requestable product.

Setting	Description
Internal product names	Text box for internal product name.
Website	Text box for the application's URL.
Link to documentation	Text box for the documentation path.
Description	Text box for entering a reason for the new application.
Comment	Text box for tips and information.
IT Shop	If set, the application is available through the Web Portal. The application can still be assigned directly to employees and hierarchical roles.
Only for use in IT Shop	If set, the application is only available through the Web Portal. The application may not be assigned directly to hierarchical roles.
Disabled	If set, the application is disabled.

To add a new resource

1. Open the menu **My Responsibilities | Other Services** and click **New resource**.

2. Configure the following settings for the new resource and click **Save**.

Table 47: Settings and data for new resources

Setting	Description
Resource	Text box for naming the resource.
Resource type	Link for selecting the resource type.
Description	Text box for entering a reason for the new resource.
IT Shop	If set, the resource is available through the Web Portal. The resource can still be assigned directly to employees and hierarchical roles.
Only for use in IT Shop	If set, the resource is only available through the Web Portal. The resource may not be assigned directly to hierarchical roles.
Service item	Link for selecting a new requestable product.

Claiming Ownership of a Group

ⓘ **NOTE:** This function is only available when the module Identity Management Base Module or Target System Base Module is installed.

You can claim ownership of a group in **Claim Ownership** under the **My Responsibilities** menu. The groups available for selection, do not have any managers. Authorized users can take on responsibility for these groups. If you claim ownership for a group, you are accountable for the interests of that group. For example, you decide about memberships within your group.

To claim ownership of a group

1. Open the menu **My Responsibilities | Claim Ownership** and select a group using the **Assign** link.

   ⓘ | **NOTE:** If you want to claim ownership for more groups, click **Claim Ownership** in the **Claim Ownership** view.

2. Click **Claim ownership**.

   Your settings are saved.

To change you ownership group

1. Select a group in the **Claim Ownership** view with the **Change** link.

2. Click **Claim ownership**.

   Your settings are saved.

Adding and Deleting Entitlements to Organizations, Business Roles and System Roles

ⓘ | **NOTE:** This function is only available when the module Identity Management Base Module, Business Roles Module or System Roles Module is installed.

Entitlements are items to which an employee belongs or is assigned, such as groups, accounts, roles, applications, and so on. You can add entitlements to organizations or roles for which you are responsible, and have the required access. The types of entitlements available depend on the systems in use in your company. When you add an entitlement, it is treated like a request, and you must process it using your cart. There are two ways for an employee to obtain entitlements.

- By making a request which is approved.
- Indirectly, by being assigned a role or belonging to an organization that has been assigned the entitlement.

ⓘ | **NOTE:** In order to set permissions for organizations, business or system roles in the **Requests** menu, the appropriate settings have be made in the Manager.

To add entitlements

1. Perform one of the following tasks.

   a. Open the menu **My Responsibilities | Organization** and select the organization you want.

   b. Open the menu **My Responsibilities | Business roles** and select the business role you want.

   c. Open the menu **My Responsibilities | System roles** and select the system role you want.

2. Select the **Entitlements** tab and click **Add a new entitlement**.

3. Select an entitlement type and select the entitlement you want using **Assign**.

4. Click **Request**.

   Your shopping cart appears. For more information, see Using your Shopping Cart to Submit your Requests on page 44.

To view currently assigned report subscriptions

After you have added "Subscribable reports" as a new entitlement and sent your shopping cart, the assigned subscribable report is displayed on the **Entitlements** tab. The report is shown in the corresponding menu item as a **Subscribable reports** shape on the **Overview** tab depending on whether you have allocated the "Subscribable report" for an organization, a business role or a system role.

- Perform one of the following tasks.

    a. Open the menu **My Responsibilities | Organization** and select the organization you want.

    b. Open the menu **My Responsibilities | Business roles** and select the business role you want.

    c. Open the menu **My Responsibilities | System roles** and select the system role you want.

    The **Overview** tab is displayed by default. The **Subscribable reports** shape contains the report and you can use the link to view more information.

The view- OR -

- Click on the user name in the header and select **My Settings** from the menu.

- Select the **Reports** tab and mark the report subscription in the list.

To delete an entitlement

1. Perform one of the following tasks.

    a. Open the menu **My Responsibilities | Organization** and select the organization you want.

    b. Open the menu **My Responsibilities | Business roles** and select the business role you want.

    c. Open the menu **My Responsibilities | System roles** and select the system role you want.

2. Select the **Entitlements** tab and check the required entitlement (multi-select is available).

3. Click **Remove entitlements**.

Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services

ⓘ **NOTE:** This function is only available when the module Identity Management Base Module, Business Roles Module, System Roles Module or Target System Base Module is installed.

You can add members to roles, organizations, and entitlements for which you are responsible and have the required access. This is an alternative to making a request for membership on behalf of an employee.

To request new membership

1. Perform one of the following tasks.

    a. Select **My Responsibilities | Organization** and select the organization you want.

    b. Select **My Responsibilities | Business roles** and select the business role you want.

    c. Select **My Responsibilities | System Entitlements** and select the system entitlement you want.

2. Select the **Memberships** tag and click **Request memberships**.

3. Select the employees you want (multi select is permitted) and click **Add to shopping cart**.

   Your shopping cart appears. For more information, see Editing Requests within your Shopping Cart on page 45.

To delete a membership

1. Perform one of the following tasks.

   a. Select the menu **My Responsibilities | Organization** and select the organization you want.

   b. Select **My Responsibilities | Business roles** and select the business role you want.

   c. Select **My Responsibilities | System roles** and select the system role you want.

2. Select the **Memberships** tab enable the check box next to the employee you want (multi select is permitted).

3. Click **Delete memberships**.

   This requests the membership deletion and it is added to the shopping cart. Your shopping cart appears. For more information, see Using your Shopping Cart to Submit your Requests on page 44.

Editing Master Data of Business Roles, System Roles and other Services

ⓘ **NOTE:** This function is only available if the module Business Roles Module or System Roles Module is installed.

Depending on you responsibilities and approvals, you can change your responsibility properties. For example, you can change the name of a department to make it easier for your staff or add managers for sharing data.

To edit your responsibility properties

1. Open the menu **My Responsibilities** and select an item from the submenu.

2. Select the tab **Master data**.

3. Make the following changes and click **Save**.

   The setting vary and are dependent on the selected object type.

Table 48: Settings and master data

Setting	Description
Object type	Text box for the object type name.
	The text box identifier depends on the selected object type.
Short name	Text box for a name abbreviation.
Internal name	Text box for internal name.
Role classes	Link for selecting the role class.
Parent business role	Link for selecting the parent business role.

Setting	Description
Role type	Menu for selecting the role type.
Manager	Link for selecting an employee as manager.
	By default, the logged in user is assigned as the manager. The business role is displayed with the manager responsible.
Deputy manager	Link for selecting the deputy manager.
Attestors	Link for selecting the parent business role.
Department	Link for selecting the department.
Location	Link for selecting the location.
Role approver	Link for selecting an application role as approver.
Role approver (IT)	Link for selecting an application role as approver (IT).
Description	Text box for entering a reason for the new business role.
Comment	Text box for tips and information.

Viewing Pending Attestation Cases for Organizations, Business Roles and System Entitlements

You can view pending attestation cases for the organizations, business roles and system entitlements that you manage.

To view pending attestation cases of certain responsibility

1. Perform one of the following tasks.

    a. Open the menu **My Responsibilities | Organization** and select the organization you want.

    b. Open the menu **My Responsibilities | Business roles** and select the business role you want.

    c. Open the menu **My Responsibilities | System entitlements** and select the system entitlement you want.

2. Select the **Attestations** tab.

    Four more tabs are shown in the view.

3. Select a tab.

    Only cases of a particular attestation type are shown, depending on your choice of tab.

4. Select an attestation case.

    This displays details of the selected case in the detailed content view. You can approve the attestation case if you have the necessary permissions. You can display other approvers for pending attestation cases and send a reminder to them.

Sending a Reminder to Attestors

You can send a reminder to attestors who are assigned to pending attestation cases.

To send a reminder to the attestors

ⓘ | **NOTE:** Only attestation cases with the status **Pending** can send a reminder to attestors.

1. Select the attestation case.

    For more information, see Viewing Pending Attestation Cases for Organizations, Business Roles and System Entitlements on page 83.

2. Click **Send reminder** and write a message to the attestators in the **Send a reminder mail** dialog box.

3. Click **OK** to confirm.

Adding Tags for Service Items

You can add tags if you are the product owner and the service item can be requested in the IT Shop. Tags help he requester to find the service item for a request, faster. You can search within the **Request** menu or with the global search in the Web Portal. For more information, see Requesting through the Search Function on page 35.

Tags can be added in the Manager as well as in the Web Portal. Add tags in the as a product owner.Web Portal For more detailed information, see the Dell One Identity Manager IT Shop Administration Guide.

To add a tag for a service item

1. Open the menu **My Responsibilities** and select an item from the submenu.

2. Select the tab **Overview** and click on the object name in the shape **Service item**.

3. Select the **Tag** tab on the object's page and click **New tag**.

4. Enter the new tag and other information about the tag in the **Create a new tag** dialog box.

5. click **Save**.

    You can add more tags for the object.

Managing Roles

Managing role basically means managing object types. Object types are divided into business roles, departments, cost centers and locations.

Role management is separated into the following functionality.

-   Comparing and merging roles
-   Splitting a role
-   Restoring Deleted Roles

ⓘ | **NOTE:** Only roles you own or manage can be merged. As business role administrator, you can manage all business roles but no other object types. As administrator of other object types, you can manage departments, cost centers and locations.

Comparing and Merging Roles

You can compare and merge any combination of role types. For example, you can compare the properties of a business role and a department, take the properties you want from them and merge them.

ⓘ **NOTE:** You can only compare and merge roles that you own. or you are an administrator.

To compare and merge roles

1. Open the **My Responsibilities** menu and select the menu item for the object type you want to compare.

2. Mark the object types in the list and click **Compare and merge** in the overview of the selected object type.

   This opens a dialog box. the view **Select a comparison role**.

3. Select a second role in the **Compare and merge** view using **Assign** next to **Object type**.

   ⓘ **NOTE:** If a role is already selected, user **Change** to edit the selection.

   Memberships and entitlements of the selected roles containing the following information are listed:

   Table 49: Overview of the selected roles' assignments

Column	Description
Object	Display name of the assigned entitlement or membership, which occurs in one of the selected roles.
Type	Type of the entitlement or membership.
Name of the source role	Assignment type if the entitlement or membership. The following assignment types are available. • Direct • Inherited • Requested • Dynamic • Not assigned For more detailed information about "Basics for Assigning Company Resources", see the Dell One Identity Manager Identity Management Base Module Administration Guide.
Name of the second role	See "Name of the source role".
Comparison	Name of the role with this assignment.

4. View the assignments of both roles and click **Merge the selected roles**.

   ⓘ **NOTE:** Use the filter function, which is available on nearly every column, to make the list of assignments clearer. For more information, see Using a Filter on page 23.

   The **Verify** view is active. This lists the actions that need to run to merge the roles.

5. Verify the suggested changes and enable/disable the actions, which should be either taken or not taken into account when the roles are merged. Click **Next**.

Save changes to the script. This opens the **Results** view.

6. Close the dialog box **Compare and Merge** dialog box.

   If you have transferred all the properties of the second role by merging, this role is removed from the overview.

Detailed information about this topic

- Managing Roles on page 84

Splitting a Role

The original idea behind splitting a role is to take assignments from role A and transfer them to role B. An example of role splitting could be, if memberships assigned to role B have less entitlements as memberships assigned to role A.

By splitting role A assigned memberships and individual entitlements of role A can be retained, moved or copied to role B.

Any combination of role types is allowed.

To split a role

1. Open the **My Responsibilities** menu and select the menu item for the object type you want to compare.

2. Mark the object types in the list and click **Split** in the overview of the selected object type.

   This opens a dialog box. The **New role data** view is shown.

3. Configure the following in the **New role data** view and click **Next**.

   Fields marked with * are compulsory.

   Table 50: Settings in the view "New role data"

Role type	Setting	Description
All	Type of the new role	Menu for selecting a type for the new role. The following object types are available in the Web Portal.
All	Department / Business role / Cost center / Location *	Text box for the new role's name. A name must be entered for every role type.
All	Short name	Text box for entering a short name for the role. This is compulsory (*) for the role type 'cost center'.
Department	Object ID	Text box for an object ID for the new role.
Location / business role	Location	Text box for entering a location.
Business role	Internal name	Text box for an internal name for the business role.
Location	Name	Text box for entering the location's name.

Role type	Setting	Description
Department / Business role / Cost center / Location	Manager	Control for selecting a manager.
Department	Deputy Manager	Control for selecting a deputy manager.
Business role	Role class *	Role class menu.
Business role / Cost center / Location *	Deputy manager	Control for selecting a deputy manager. The option **Employees do not inherit** is also available.
Department	Parent department / Attestor / Cost center / Role approver / Role approver (IT)	Controls for selecting the respective settings.
Business role	Parent business role / Role type / Role approver / Role approver (IT)	Controls for selecting the respective settings.
Cost center	Parent cost center / Attestor / Department / Role approver / Role approver (IT)	Controls for selecting the respective settings.
Location	Parent location / Attestor / Department / Cost center /Role approver / Role approver (IT)	Controls for selecting the respective settings.
All	Description	Text box for more detailed description.
Business role	Comment	Text box for additional comments.

After clicking **Next**, the **Splitting** view is opens. The view is divided in to the sections **No change**, **Copy to new role** and **Move to new role**, which a differentiated by color.

All memberships assigned to role A are listed in **Copy to new role**. Assigned members are copied to the new role by default. This means, they are contained in role A and in role B after splitting.

However, You can copy or move these members to the new role or retain them. The following edit options are available. Edit option also apply to assigned entitlements.

Table 51: Assignment Edit Options and Effects on Role A and Role B

Section	Action	Significance
No change / Copy to new role / Move to new role	Retain assignment	The entitlement / membership remains in role A.
	Retain and copy to new role.	The entitlement / membership is copied to role B. It is now in role A and in role B.
	Move to new role	The entitlement / membership is moved to role B. It is now in role B but not in role A.

4. Configure the assigned memberships and entitlements by navigating to an object, an employee in **Copy to new role**, for example, and clicking ▼.

5. Select one of the following actions from the menu and click **Next**.

    a. Keep this assignment

    b. Keep and copy to new role.

    c. Move to the new role

   This opens the **Verify** view and lists the actions.

6. You can deselect individual actions if you do not want to run them all. Click **Next**.

   Save changes to the script. This opens the **Results** view.

7. Close the dialog box.

Detailed information about this topic

- Managing Roles on page 84

Restoring Deleted Roles

Another function for managing roles is restoring deleted roles. An example of a deleted role could be roles that have been sorted out during merging.

To restore deleted roles

1. Open the **My Responsibilities** menu and select the menu item for the object type you want to compare.

2. Click **Restore a deleted role** in the view displaying the list of object types.

   This opens a dialog box. The view **Select deleted role** is enabled and lists all the deleted objects.

   ⓘ | **NOTE:** You can set a date in order to limit your search for deleted roles.

3. Select the desired role and click **Next**.

   Multi-select is possible. The view **Verify** appears and lists the actions that will be run on restore.

4. You can deselect individual actions if you do not want to run them all. Click **Next**.

5. Close the dialog box.

Detailed information about this topic

- Managing Roles on page 84

Assigning Owners

In the **My Responsibilities | Assign Ownership** menu, you can assign owners to business objects. A wizard is available to help you make the assignments.

You can assign ownership to the following business objects.

- Device
- System entitlement

To assign an owner to a device

1. Open the menu **My Responsibilities | Assign Ownership** and click **Device**.

   This opens a dialog box. The view **Select a device** is active.

2. Click **Assign** next to the **Device** field and select a device from the list.

   This selects the device and displays details about it, for example, device model, workdesk and cost center.

3. Click **Next** and select one the options in the **Select the new owner**'s view.

   a. Select one of the calculated possible owners

   In this case, you do not have to change any other settings.

   b. Select another owner.

   In this case, select an employee from the displayed list.

4. Click **Next** and then **Close** in the **Results** view.

To assign system entitlements to an owner

1. Open the menu In the **My Responsibilities | Assign Ownership** menu and click **System entitlements**.

   This opens a dialog box. The view **Select a system entitlement** is active.

2. Click **Assign** next to the **System entitlement** field and select a group from the list.

   This selects the group and displays details about it, for example, group type or target system.

3. Click **Next** and select one of the options in the **Select the new owner** view.

   a. Select one of the calculated possible owners

   In this case, you do not have to change any other settings.

   b. Select another owner.

   In this case, select an employee from the displayed list.

4. Click **Next** and then **Close** in the **Results** view.

Managing Employees

You can add new employees to the system using this menu item. This function is mainly designed for adding external employees. For example, subcontractors who are not entered in the human resources department. Data from new employees 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.

Adding Employees

To add a new employee

1. Open the menu **My Responsibilities | People** and select **Add a new employee**.

2. Enter the required data for the new employee and click **Save**.

   Fields marked with * are compulsory. The combination of last name and first name is checked on saving.

   There are different use cases that require different input sequences. The following tables layout the user cases and the respective input sequences.

Table 52: Use Cases and Input Sequences when Adding a New Employee

Use Case	Input Sequence
If this combination of first and last name does not exist, you will be prompted to save the changes.	a. Confirm the prompt with **OK**. This adds the new employee. b. Save the changes.
If this combination of first and last name already exists, they are listed in the view **Other employees with similar properties**. In this case, you have two possible options.	
If the employee you want to add is already in the list, you can select this data record and edit it. Proceed as follows.	a. Mark the employees in the list whose data you want to use and click **Update employee data**. This displays a message and you are prompted to save the changes. b. Confirm the prompt with **OK**. The new employee data is added with the existing data. You can edit or change the data. c. Save the changes.
Another option is to add new data despite the duplicate data record.	a. Click **Add a new employee**. A message is displayed and you are asked whether you want to add a new employee. b. Confirm the prompt with **OK**. This adds the new employee. c. Save the changes.

Editing Employee Data

To view and edit employee data

1. Open the menu **My Responsibilities | People**.

2. Use a filter and then mark the item you want in the result list.

3. Make your changes on the **Master data** tab and click **Save**.

> ⓘ | **TIP:** The tabs **Overview**, **Requests**, **Risk** and **History** are the same as the tabs under the menu **Auditing - Employee Details**.

Detailed information about this topic

- Using a Filter on page 23
- Editing Master Data of Business Roles, System Roles and other Services on page 82
- Auditing - Employee Details on page 120

Editing Employee Memberships

To view and edit employee memberships

1. Open the menu **My Responsibilities | People**.
2. Use a filter and then mark the item you want in the result list.
3. Select the **Entitlements** tab and set the option **Edit memberships**.
4. Mark the membership whose details you want view in the detailed content view.
5. Enable the check box in front of the memberships if you want to delete the membership and click **Delete membership**.

Editing Employee Delegations

To view and edit employee delegations

1. Open the menu **My Responsibilities | People**.

   > ⓘ | **NOTE:** There is a filter to help you search for a particular employee.

2. Click **Select** next to the employee you want and click the **Entitlements** tab to view assigned entitlements and memberships.
3. Select the option **Edit delegations** to view a table with roles, which are not delegated and set the option for the role you want to delegate to the employee.

   You can view more information in the detailed content view.

   > ⓘ | **NOTE:** If you have enabled one or more roles, the option **New delegation** becomes available. Click **Delegate all** if you want to delegate all roles in the table.

4. Click **New delegation** and enter the data required in the **New Delegation** dialog box.
5. Save the changes.

Viewing Entitlements and Memberships of an Employee

To view employee entitlements and memberships at a glance

1. Open the menu **My Responsibilities | People**.

2. Use a filter and then mark the item you want in the result list.

3. Select the **Entitlements** tab to view assigned entitlements and memberships.

4. Select the **Overview** tab to view all memberships and entitlements at a glance.

Viewing an Employee's Risk Index

To view an employee's risk index

ⓘ **NOTE:** For more detailed information, see the Dell One Identity Manager Risk Assessment Administration Guide.

1. Open the menu **My Responsibilities | People**.

2. Use a filter and then mark the item you want in the result list.

3. Select the **Risk** to view the risk index assessment view and click **View risk functions**.

Viewing Details of an Entitlement Assignment to an Employee

To view details of an entitlement assignment to a specific employee

1. Open **My Responsibilities | People** and select the employee.

2. Select the **Entitlements** tab.

   ⓘ **NOTE:** The option **Edit memberships** must be set.

3. Mark the entitlement you want and click the icon next to **Analysis for...** in the detailed content view, ▶.

   More entries are displayed. Like, the origin of the entitlement and related details.

Viewing an Employee's Pending Attestation Cases

To view details of pending attestation cases for a specific employee

1. Open **My Responsibilities | People** and select the employee.

2. Select the **Attestations** tab.

   Four more tabs are shown in the view.

3. Select a tab.

   Only cases of a particular attestation type are shown, depending on your choice of tab.

4. Select an attestation case.

   This displays details of the selected case in the detailed content view. You can approve the attestation case if you have the necessary permissions. You can display other approvers for pending attestation cases and send a reminder to them.

Sending a Reminder to Attestors

You can send a reminder to attestors who are assigned to pending attestation cases.

To send a reminder to the attestors

ⓘ | **NOTE:** Only attestation cases with the status **Pending** can send a reminder to attestors.

1. Select the attestation case.

   For more information, see Viewing an Employee's Pending Attestation Cases on page 92.

2. Click**Send reminder** and write a message to the attestators in the **Send a reminder mail** dialog box.

3. Click **OK** to confirm.

Assigning a New Manager to an Employee

To assign an employee to a new manager

1. Open **My Responsibilities | People** and select the employee.

2. Select the **Master Data** tab and click **Assign to new manager**.

3. Select a new manager using the **Change** link.

4. Enable the option in the **Assign to new manager** view and set a time and date from which the new manager takes effect.

   ⓘ | **NOTE:** If the employee with the new manager already has approved requests or entitlements, they are deleted automatically on this date. If you want the employee to retain these requests or entitlements when transferring to the new manager, disable the checkbox **Delete assignment on the effective date** or **Cancel on the effective date** respectively.

5. Click **Send** and confirm the prompt with **OK**.

   Your changes are saved and the message **Your manager change request has been submitted.** is displayed in the employee's **Master data**.

   ⓘ | **NOTE:** Your request to change managers is presented for approval in the **My Actions | Pending Request** menu of the approver responsible.

Detailed information about this topic

- Approving Assignment of a New Manager on page 55
- Viewing Approval History on page 59
- Processing Pending Requests on page 51

Comparing an Employee's State

You can compare the current state of an employee with their state in the past in the **History** view. This compares attributes, which have changed within a specified time period. You specify the time period yourself in the date control provided.

This comparison is also available for company structures. For more information, see Comparing an Company Structure's State on page 74.

To run a comparison of an employee's status

1. Open **My Responsibilities | People** and select the employee.

2. Select the **State comparison** tab on the **History** tab.

3. Click 📅 and ✅ and select a date and time with which you want to compare the employee's current state.

   All the attributes for this employee are displayed in a list. By default, all attributes are selected.

   > ⓘ **NOTE:** You can apply a filter to all columns in the view. For more information, see Using a Filter on page 23.

Managing Devices for Employees

The menu **My Responsibilities | Devices** not only shows you your own devices but also your staff. You can see, which devices are assigned to your staff and change the assignments. You can also assign new devices to your staff.

To change a device assignment

1. Open the menu **My Responsibilities | Devices** and select the entry you want to change from the list.

2. Click **Change** next to **Used by** in the **Master data** tab and select another employee from the list.

3. Save the changes and confirm the prompt with **Yes**.

Detailed information about this topic

- Viewing, Editing and Adding Devices on page 69

Compliance Rule Violations by Direct Reports

In the menu **My Responsibilities | People** you can view your staff's rule violations.

To view rule violations by direct reports

- Open the menu **My Responsibilities | People** and click **Rule violations**.

  In the view, **Compliance rule violations by direct reports**, you can see the rule violations caused by your supervised employees. The following information is listed in the view.

Table 53: Columns in the View "Rule Violations by Direct Reports"

Columns	Description
Employee	Name of the supervised employee
Rule violation	Unique rule violation ID.
Checked	Shows whether the rule violation was tested.
Exception is approved	Shows whether an exception was approved for the rule violation.
Risk index (calculated)	Shows the calculated risk index.
Risk index (reduced)	Shows the reduced risk index.
Approval date	Shows the approval date, if the rule violation was already checked.
Reason	Shows a reason for the approval decision about the rule violation.

You can select other columns to view using the **Additional columns** link. The following columns are available.

Table 54: Additional Columns for the view "Compliance rule violations by direct reports"

Columns	Description
Approver	The name of the approver checking the rule.
Valid until	Date specifying for how long the rule violation applies.
Standard reason	Default reason available for all rule violations. Multiple use is possible.

Accessing Other Applications

You may be able to access other applications, as configured by your system administrator. This provides you with a shortcut to other web applications deemed of value by your company.

ⓘ **NOTE:** If you are a system administrator, and would like to add applications, see the Dell One Identity Manager Web Designer Reference Guide.

To access other web applications from the One Identity Manager Web Portal

- Open the **Applications** menu and choose the desired web application.

   The application may appear within the Web Portal, or in a separate window, depending on how the system administrator configured it.

Getting Information Using Views, Reports and Statistics

The One Identity Manager provides a lot of information about you, your staff, other resources and previous handling. You access to different statistics, views and reports depends on your role and access rights. In the following three sections, you will discover how to get this information.

Detailed information about this topic

- Discovering your Statistics on the Start Page
- Using Views to Get Information
- Generating Reports

Using the Help

You can use the guide as well as online help to answer questions about the Web Portal. The online help is available in the web application, for example.

To call up help in the Web Portal

- Click in the header and then **Help**.

    The Dell One Identity Manager Web Portal User Guide is opened as online help.

Information about the Current Connection

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

ⓘ **NOTE:** It is only possible to view the information about the database connection. You cannot make changes to the data.

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

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

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

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

To open the "Connection" dialog box.

1. Click ⓘ in the header and then **Connection**.

2. Select the tab for the information type you want to view in more detail.

Discovering your Statistics on the Start Page

Statistics are graphical summaries of the information pertaining to you. The data on the start page in the main sections **My Identity** and **Access Governance** are brought up-to-date every day. You can customize the data you see in the Info System by selecting the objects you want to include, and which statistics you want to show for each object. Checking your statistics regularly can help you understand any issues that need addressing. If not all the statistics are displayed on the start page, you can use ❯ on the right to "leaf" through all available statistics in each section. For more information, see What Statistics are Available? on page 100.

Detailed information about this topic

- Statistics on page 97
- Heatmap on page 98
- What Statistics are Available? on page 100

Statistics

Graphical representation of data is depicted in diagrams. Heatmaps also provide data in graphical form. For more information, see Heatmap on page 98.

Table 55: Icons Used in Diagrams

Icon	Meaning
⚠	The value in this statistic is in the balance. It is neither critical nor compliant. You should keep an eye on this value or statistic, respectively.
→	This value has not changed. The date of last change is shown when you mouse over.
✔	This icon verifies that the value in this statistic compliant. The arrow icon displayed in combination with this icon, is also green and provides more detailed information about changes to the value.
✖	This icon indicates that the value in this statistic is in the critical range. The arrow icon displayed in combination with this icon, also means critical and provides more detailed information about changes to the value.
↗	This arrow icon shows the value has increased since the last change. The value is still in a compliant range. The difference since the last change is shown when you mouse over.

Icon	Meaning
↘	This arrow icon shows the value has increased since the last change. The value is still in a compliant range. The difference since the last change is shown when you mouse over.
↗	This arrow icon shows the value has increased since the last change. The value is in the non-compliant range and more critical than before. The difference since the last change is shown when you mouse over.
↘	This arrow icon shows the value has increased since the last change. The value is in the non-compliant range but better than before. The difference since the last change is shown when you mouse over.

To display a statistics view

ⓘ **NOTE:** Hyper Views, heatmaps and statistics have different behavior in the desktop view as opposed to the mobile view. For more information, see Heatmaps and Statistics for Mobile Devices on page 33.

1. Select either **My Identity** or **Access Governance** in the main section on the start page.

   All the roles and organizations for which you are responsible are displayed on the start page. These roles or organizations are divided into their associated subgroups.

2. Click the role or organization you want to see in more detail.

   Depending on your selection, you are shown statistics either in form of a table or a heatmap. There are also, however, roles or organizations, which take you to a page with source data.

To view source data from a role or organization

ⓘ **NOTE:** You can only view source data for certain roles and organizations. You can view a heatmap or statistics, with graphical representation, through certain roles or organizations.

1. Select either **My Identity** or **Access Governance** in the main section on the start page.

   All the roles and organizations for which you are responsible are displayed on the start page. These roles or organizations are divided into their associated subgroups.

2. Click the role or organization you want to view in more detail, for example, departments without managers.

   This displays a view with the corresponding data.

To customize the information displayed on a statistics view

- Apply a filter to the statistic view.

   This opens a dialog box for the selected filter. For more information, see Tips for using the Web Portal on page 18.

   ⓘ **NOTE:** The filter function is not available for all statistics.

Heatmap

The heatmap in the Web Portal presents roles and organizations as colored squares. They are intended to help you quickly visualize particularly prominent values within a large amount of data and to comprehend them at a glance. The size of the rectangles corresponds to the relative size of the role or organization. The more employees you have in a company's structure, for example, the larger the rectangle in the view.

ⓘ **NOTE:** An overview of the part of the company structure under your responsibility is either displayed on the **My Identity** or the **Access Goverance** main page.

The rectangle colors correspond to a selectable linked in data value and range from red to green, where red stands for a value tending to required more attention. Red signals, for example, a lot of compliance rule violations or employees with high risk indexes. The color 'yellow' stands for an average, which can also mean that there has been no changes to this company structure since the last analysis. The heatmap not only provides a clear overview of the current data, it also provides another useful function by making a historical comparison to previous data.

You can see the following risky results or properties in a heatmap.

- Policy violations

- Average number of permissions per employee

- Highest employee risk index

- Average employee risk index

- Rule violations

- Highest resource risk index by host

ⓘ **NOTE:** Hyper Views, heatmaps and statistics have different behavior in the desktop view as opposed to the mobile view. For more information, see Heatmaps and Statistics for Mobile Devices on page 33.

To view data from a role or organization

ⓘ **NOTE:** Without having set any preferences, the color map is displayed as a data value, for example, for the number of compliance rules when you open it.

1. Select either **My Identity** or **Access Governance** in the main view on the start page.

2. Click on the role or organization in form of a heatmap, if it exists, that you want to view more closely.

   ⓘ **NOTE:** In the first field, you can set the size of the square. Available settings are **Data size** and **Unisize**.

3. Limit your selection by selecting one or more objects with the link **Change**.

4. Confirm your selection by clicking **Close**.

   You selection is displayed to the left of the **Change** link.

To view data for a specific time period

- Select the entry you want from the second field, for example, month-to-date changes.

   The data is displayed in the heatmap according to your selection.

To limit the size of the data

- Click on one of the slide rulers in the scale an the bottom of the view to limit the data size.

   ⓘ **NOTE:** You may be shown up to 500 data sets graphically.

To obtain more information about individual roles or organizations

1. Click on the rectangle in the view after you have made your settings and the Web Portal has adjusted the view to them.

Another shape is displayed for the rectangle with additional information.

> (i) **TIP:** You also obtain additional information about the role or organization of you choice when you mouse over the corresponding rectangle. This information is not so comprehensive and is there to provide initial orientation within the heatmap.

2. Perform one of the following tasks.

   a. Click on one of the clickable items to obtain more information.

   b. Select other information using the link **Display object details**.

A view with detailed information, spread over several tabs, is displayed for the square you click on.

What Statistics are Available?

The statistics and heatmaps you see in the Web Portal depend on your roles and permissions. Only statistics relevant for you are available on the start page of the following main content pages.

- **My Identity**
- **Access Governance**

Statistics can be customized to display the objects and statistics that interest you. You can also sort and filter statistic information, and export it to a report. For more information, see Discovering your Statistics on the Start Page on page 97.

Detailed information about this topic

- High Risk Overview on page 100
- Compliance on page 101
- Risk on page 101
- Policies on page 102
- Organizations on page 103
- IT Shop on page 103
- Attestations on page 104
- Target systems on page 104

High Risk Overview

You will find an overview of critical objects in the **Access Governance** in the menu **Compliance**. This overview lists high risk objects and divides them up into different groups that can be expanded and collapsed. Each of the groups displays resources with the highest risk factor, which you manage. Risk indexes are calculated on for employees, user accounts, system roles, structures, organizations and business roles. Risk indexes are calculated for employees, user accounts, system roles, IT Shop structures, organizations and business roles, file system and SharePoint® resources. Object have risk values, which provide the risk index when combined with risk index functions. You can view the following information in the statistic **High Risk Overvew**.

- Breakdown for of the highest risk items for each type
- For more information on risk function calculators, see Modifying Risk Calculators.

Compliance

ⓘ | **NOTE:** This function is only available when the module Compliance Rules Module is installed.

The Manager can be used to define rules that maintain and monitor regulatory requirements and automatically deal with rule violations. Rules are used for locating rule violations and to prevent them.

You will find statistics about compliance rules on the **Access Governance** start page. Statistics are available on the following topics.

Table 56: Overview of compliance rule statistics

Statistics	Description
Pending rule violations	Show all types of rule violations.
Compliance violations	Shows compliance violations.
	This statistic is available for different company structures.
	• Department
	• Location
	• Cost center
	• Business role
Compliance rule violations by rule	Shows compliance rule violations for each rule.
New rule violations	Show new rule violations.
	This statistic is also available for new rule violations in recent months.
Overdue rule violations	Shows overdue rule violations.
Assignments that contribute to violations	Show assignments, which contributed to violations.
Last approvals granted (rule violations)	Show the last granted approvals, which contributed to rule violations.
Cost centers with increased violations	Show the cost centers, which stand out due to a high rate of violations.
	This statistic is also available for other company structures.
	• Departments
	• Locations
Last approvals (rule violations)	Show the last approvals, which contributed to rule violations.

For more information, see Managing Compliance on page 126.

Risk

There are various statistics available to you for risk assessment. You will find these statistics on the **Access Governance** start page.

Table 57: Risk assessment statistics

Statistics	Description
Number of active employees with a risk index of more than 0.5	Shows the number of active employees with a risk index more than critical value.
Highest person risk index by department	Show the highest risk index of all employees by department. This statistic is also available for other company structures. • Location • Cost center • Business role
Average person risk index by department	Shows the average risk index of employees by department. This statistic is also available for other company structures. • Location • Cost center • Business role
Employees by risk index	Show all employees in groups of risk index in the same range.

Policies

Other, different statistics are available for company policies. You will find these statistics on the **Access Governance** start page.

Table 58: Company policy statistics

Statistics	Description
Pending policy violations	Shows pending policy violations.
Overdue policy violations	Shows overdue policy violations.
Policy violations by department	Shows policy violations by department. This statistic is available for different company structures. • Location • Cost center • Business role
New policy violations	Shows new policy violations. This statistic is also available for new policy violations within the last month.
Policy violations (actual)	Shows current policy violations. This statistic is also available for new policy violations within the last 7 days.

Statistics	Description
Policy violation approval rates	Shows the approval rate for policy violations.
Last approvals (policy violations)	Show the last approvals, which contributed to policy violations.
Last approvals granted (policy violations)	Show the last granted approvals, which contributed to policy violations.

Organizations

These statistics are on the **Access Governance**'s start page. The following statistics are displayed for departments you manage.

- Information about employee accounts
- Information about employees
- Rule violations
- Information about pending requests
- The top roles and entitlements

For more information, see Managing Company Structures on page 72.

IT Shop

The shop is the mechanism employees use to make requests. These statistics are displayed in the **Access Governance** main content and help to answer the following questions.

- Which products are the most popular, both by product owner and by shop
- How fast requests are processed
- Request frequency over time

Table 59: Statistics about IT Shop structures

Statistics	Description
Pending Requests	Displays all pending requests.
Open requests by service category	Displays all pending requests by service category.
	This statistic contains other criteria.
	- By next approver
	- By recipient
Last approvals granted (Shop)	Shows the last approvals granted for requests.
New requests	Shows new requests.
Number of requestable products	Shows the number of products that can be requested.
Denied requests by service category	Shows denied requests by service category.
Average request processing time by shop	Show the average processing time of a request by shop.

Statistics	Description
Top 10 requested products by shop	Shows the top 10 requested products by shop.
	This statistic is also available for the top 10 requested products by product owner.
Request frequency (12 months)	Shows the frequency of requests within the last 12 months.
	This statistic is also available for the frequency of requests within the last 12 months by owner.

For more information, see Managing Company Structures on page 72.

Attestations

There are a number of statistics available to you for attestation cases. You will find these statistics on the **Access Governance** start page.

Table 60: Attestation case statistics

Statistics	Description
Pending attestation cases	Displays all open attestation cases.
	This statistic contains other criteria.
	- By policy
	- By next approver
	- By framework
Attestation approval rates	Shows the approval rate for attestations.
Decided attestation approvals within / over the limit	Shows attestation approvals decisions within / over the limit.
	This statistic is also available for pending attestation cases within/over the limit.
Attestation status by type	Show attestation status by type.
Attestations	Shows all attestations.
Last approvals (attestation)	Shows the most recent attestation approval decisions.
	This statistic is also available for attestations which have been granted approval.
Overdue attestations	Displays overdue attestations.

Target systems

There are a number of statistics available to you for target systems. You will find these statistics on the **Access Governance** start page.

Table 61: Target system statistics

Statistics	Description
Pending attestation by system entitlements	Shows pending attestation by system entitlements.
Number of user accounts with a risk index of more than {0}	Shows the number of user accounts with a risk index more than specified value. This statistic is also available for the number of entitlements with a risk index more than specified value.
User accounts having risk higher {0} by domain	Shows user accounts with a risk index more than specified value by domain. This statistic contains other criteria. • Entitlements having risk higher that a specified value by domain. • Entitlements having risk higher that a specified value by department.
Employees without user accounts	Show employees without user accounts.
Entitlements without requests	Shows entitlements without a request. This statistic contains other criteria. • Active Directory® • Oracle® E-Business Suite • LDAP • SAP® R/3® • SharePoint®
Groups with / without user account assignments	Shows groups with or without user account assignments. This statistic contains other criteria. • Active Directory® • LDAP • SAP® R/3® • SharePoint® • Notes • Groups, roles and profiles with/without user account assignments SAP® R/3®
Inactive employees with enabled user accounts	Shows inactive employees with enabled user accounts.
Locked user accounts of enabled employees	Shows locked user accounts of active employees.

Using Views to Get Information

A variety of views are available to you, depending on the type of information you need and your access permissions. The following information is available.

- Information about You and Your History
- My Business Ownerships
- Auditing Information

In many cases, you are able to customize the view to maximize its usefulness, and export the information to a report. For more information, see Tips for using the Web Portal on page 18. Many views share common pages. For more information on the tables, see Description of Commonly Used Tabs in Views on page 109.

Information about You and Your History

You can view information about yourself, your responsibilities and the history of your previous actions.

Your Overview

The overview provides you with a general look at your memberships, responsibilities and entitlements on two pages.Manager The starting point for the Hyper View is the **Person** shape. This displays information about yourself. For example:

- Form of address
- Full name
- Phone
- User account
- Default email address
- Primary cost center
- Manager

ⓘ | **NOTE:** The number of shapes shown in the Hyper View, depends on the entitlements and responsibilities you hold.

The information cannot be edited. If you think you are resources missing, you can request them from the **Request** menu.

To display an overview of your profile

ⓘ | **NOTE:** Hyper Views, heatmaps and statistics have different behavior in the desktop view as opposed to the mobile view. For more information, see Hyper Views and Mobile Devices on page 31.

1. Click on the user name in the header and then **My profile**.

   The **Overview** is displayed in a Hyper View.

(i) **NOTE:** A user, with other sub identities apart from a main identity in the Web Portal, can select an identity from the **Identity** menu on the **Contact Data** tab.

The selected identity is displayed as the main shape with all the other shapes are linked to it. If the selected identity is the main identity, the subidentities are displayed in a separated shape.

2. Move the shapes if you want to improve the overview to better view the details.

(i) **NOTE:** You can click on the contents some of the shapes. Use the links to go directly to the view of the selected content to see other information.

3. Click on of the links in a shape to view more information.

The number of items or the content of the shape is shown in brackets. The maximum number of entries displayed per shape is defined during project configuration in the Web Designer (default setting is 5 elements).

Contact Data

The overview **Contact Data** contains information about yourself and can also be seen by other Web Portal users in the **White pages**. For more information, see Updating your Contact Information on page 10 and Using the White Pages to Look Up Employees on page 108.

To open the "Contact Data" view

- Click on the user name in the header and then **My settings**.

The **Contact Data** tab is predefined and displayed in the **My Settings** view.

My Action History

You can see the actions you have performed or others have performed for you, in **My Action History**. For example, if you want to see when a request was approved, or by whom, you can use the history. You can filter your history on a date range to help you locate specific items. Depending on your role and access permissions, you can see the history of:

- Requests you have made:

  For more information, see Making a Request on page 35.

- Approvals and denials of other employees' requests.

- Attestation decisions.

- Approval decisions about historical rule violations.

- Policies violations you have edited.

- Roles you have delegated to your staff.

  For more information, see Delegating Roles on page 62.

To view your action history

1. Open the menu **My Action History**.

2. Select the submenu.

3. If desired, set a date range for the history.

   ⓘ | **NOTE:** You can use the search to locate specific items. For more information, see Tips for using the Web Portal on page 18.

4. Click on the available links to display more details.

Using the White Pages to Look Up Employees

The **White pages** tab lists information about all employees. You can use them to look up phone numbers, locations, or other information about employees in the Web Portal. Open the **White pages** view before you start to search for information about employees. For information on searching and filtering, see Tips for using the Web Portal on page 18.

Once you locate an employee, you will find more information such as their manager or cell phone number.

To look up an employee

1. Click ⓘ in the Web Portal header and select **White Pages**.

2. Search for the desired employee in the **White pages** view.

   For more information, see Tips for using the Web Portal on page 18.

3. Click **Overview** in the detailed content view for more details, for example, "default email address".

My Responsibilities

You can view any business ownerships that you have. The **My Responsibilities** menu shows you any of the following if you have been assigned responsibility:

- Organizations
- Business roles
- System roles
- System entitlements
- other services

In many cases, you are able to manipulate the view to maximize its value, and export the information to a report.

To view information about your responsibilities

1. Open the menu **My Responsibilities**.

2. Select the type of responsibility.

3. Select an item from the overview.

4. Examine the tabs associated with the view.

   For more information, see Description of Commonly Used Tabs in Views on page 109.

Detailed information about this topic

- Tips for using the Web Portal on page 18
- Managing "My Responsibilities" on page 71

Auditing

If you are a manager or auditor, you may have access to the **Auditing** menu. The **Auditing** menu displays a list of all items for which you are responsible. You will find this menu in the section **Access Governance**. You can use it to the check whether employees are complying to policies properly. In many cases, you are able to manipulate the view to maximize its value, and export the information to a report.

To view auditing information

1. Open the menu **Auditing**.
2. Select a submenu and if necessary an item from the menu to view the details in the overview.
3. Select the table you want to view the details if a view has multiple tables.

   For more information, see Description of Commonly Used Tabs in Views on page 109.

Detailed information about this topic

- Tips for using the Web Portal on page 18
- Auditing Activity and Managing Compliance on page 120

Description of Commonly Used Tabs in Views

Some views have multiple tabs to provide you with all of the information. They appear in the following main areas.

- My Identity
- Access Governance

The details within a tab vary slightly depending on the view. In many cases, you are able to manipulate the view to maximize its value, and export the information to a report. For more information, see Tips for using the Web Portal on page 18.

Detailed information about this topic

- Master Data on page 110
- Overview on page 110
- Permissions on page 110
- Requests on page 111
- Risk on page 111
- History on page 111
- Attestations on page 114
- Memberships on page 114

Master Data

Master data consists of the properties of the objects saved in the database. This tab is available in the **People** menu, if, for example, you wanted to look at details of an employee. If you have the right permissions you can not only view but also edit master data.

To open an employee's master data

1. Open the menu **My Responsibilities | People**.

2. Select the employee whose master data you want to view.

3. Verify the employee's data in the **Master data** view and make any changes.

4. Save the changes.

ⓘ | **NOTE:** Many items have a risk index as one of the properties. For more information about risk index and about usage, see the Dell One Identity Manager Risk Assessment Administration Guide.

Overview

The **Overview** tab is a Hyper View. The center of the Hyper View is the item you selected. All resources associated with the selected item are shown, giving you an overview of how the item fits into the system. You can click on the links and buttons in a shape. This is the way to obtain more detailed information or to navigate around within the shape.

ⓘ | **NOTE:** Hyper Views, heatmaps and statistics have different behavior in the desktop view as opposed to the mobile view. For more information, see Heatmaps and Statistics for Mobile Devices on page 33.

Table 62: Configuration options for a shape

Icon	Description
📑	Closes the shape
📑	Opens the shape
1, 2, …	Goes to the page with the select number.
▶	Goes to the last page in the shape.
◀	Goes to the first page in the shape.
5 ⌄	Sets the number of objects displayed on a shape page.

For more information, see Tips for using the Web Portal on page 18.

Permissions

The **Entitlements** tab provides you with an list of entitlements assigned to the selected item.

To view details about entitlements for an organization

- Mark an entitlement on the **Entitlements** tab to view more detailed information in the detailed content view.

For more information, see Adding and Deleting Entitlements to Organizations, Business Roles and System Roles on page 80.

Requests

This tab shows all the products that the employee has requested, or that have been requested for him or her by another employee, for example a manager.

To search for a specific approval decision by approval

1. Select the **Requests** tab.
2. Perform one of the following tasks.

    a. Use a filter and then mark the item you want in the result list.

    b. Mark the entry you want in the list.

    This displays details of the selected item in the detailed content view.

Risk

Many items have a risk index associated with them, allowing you to make a risk assessment. On the **Risk** tab, you see the factors that contribute to the risk assessment of an item. For more information, see Modifying Risk Calculators on page 128.

You can view the risk assessment for a particular employee, for example. The risk index is calculated for objects types **employees**, **user accounts**, **departments**, **locations**, **cost centers**, **business and system roles**, **IT Shop structures** and **rule violations**.

To run risk assessment for an employee or any other object type

1. Perform one of the following tasks.

    a. Select an object type, for example **People** in the **My Responsibilities** menu in the main **My Identities** view.

    b. Select the employee in **Auditing | Employee details** in the main **Access Governance** view.

2. Click the **Risk** tab.

History

You can use the **History** tab to see changes to a base object over time. It shows states and comparisons of base object attributes.

The overview is divided into the following three tabs.

Table 63: "History" tab overview

Tab	Description
Events	Displays all events affecting the base object, on a timeline.
	This tab is displayed on the **History** start page.
State overview	Displays a list of modified properties with their validity period and dates when they were changed.
State comparison	Displays the differences between in the current and selected time point.

To move back and forward on the timeline in the "Events" view.

1. Click on the timeline and hold down the left mouse key.

2. Perform one of the following tasks.

   a. Drag the marking to the left to go forward in time on the timeline.

   b. Drag the marking to the right to go back in time on the timeline.

To change the timeline view on the "Events" tab

- Turn the mouse wheel to zoom in or zoom out.

   The timeline view can vary from months to hours.

To swap table views on the "Events" tab.

- Click **Switch to table view** at the bottom of the "Events" view.

   This switches views and the same data is shown in a table. The table displays the change type, property, new and old value of the change and the date of change, amongst others. Click **Switch to timeline view** to switch back to the timeline.

To view details of an event

- Click on one of the colored elements on the timeline to view more details of this particular event.

To apply a filter to the timeline on the "Events" tab

1. Click **Filter by...** and select an entry from the following.

   Table 64: Filter option on a timeline

Filter	Description
User	Searches for events or actions associated with the given name.
	Employees with entitlements and ownerships create changes, such as adding or removing properties. You can view these actions on the timeline.
Change type	Lists all changes types, which can be selected for displaying in the timeline.
	Multi-select is possible.
Date	List all actions and events for the selected date.
Property	Lists all properties, which can be selected for displaying in the timeline.
	Properties are, for example, employee, manager or dynamic role.
	For more detailed information about assigning through dynamic roles, see the Dell One Identity Manager Identity Management Base Module Administration Guide.
	Multi-select is possible.
Display	Searches for all text data matching the given search term.
	The following settings are available.
	• All words
	• Starts with...
	• Ends with...
	• One or more words

2. Apply the selected filter with **Filter on**.

To compare the current state of the object with a state in the past

- Perform one of the following tasks.

  a. Click in the **Compare** dialog box if you clicked the event on the timeline.

     This compares the current object state is compared with the time point selected and the result is displayed on the **State comparison** tab.

  b. Select the tab **State comparison** and click 🗓 next to the text box. Select the date.

The states and comparisons displayed in the **History** overview are dependent on the type of base object selected. The following attributes can be displayed.

Table 65: Overview of Base Objects and their Attributes

Base object type	Attribute
Employee	Change of base object property
	Responsibility for an employee
	Responsibility for a department
	Responsibility for a cost center
	Responsibility for a location
	Membership in an application role
	Membership in a department
	Membership in a cost center
	Membership in a location
	Assignment to a resource
	Application assignment
	Identifying a compliance rule violation
	Assignment to a business role
	Responsibility for a business role
	Responsibility for a system role
	Assignment to a system role
	Assignment to a target system account
Department	Change of base object property
Cost center	Employee membership
Location	Assignment to a resource
Business role	Assignment to a system role

Attestations

ⓘ | **NOTE:** This function is only available when the module Attestation Module is installed.

On **Attestation** tab you can view a list of attestation cases. For each case you can see the current status and the creation date in the detailed content view. You can run the following action or get information.

- See whether the case was approved or denied.

- Obtain detailed information about the selected attestation case on the tabs **Information**, **Workflow**, **Attestation Policies** and **History** in detailed content view.

- As attestor, you can view attestors for pending attestation cases.

Memberships

The **Memberships** tab provides you with an summary of all employees that have access to the selected item.

To view an employee's membership details

- Mark an employee in **Memberships** to view more detailed information in detailed content view.

For more information, see Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services on page 81.

Usage

Roles are used to help manage assignments to employees. For example, instead of assigning many resources separately to an employee, you can add them to a role that inherits the proper assignments from a role class. A role class is the highest level, and roles can be nested in it. On the **Usage** tab, you see all role members that can be member of the selected entry. If you select a role class, you can view all the members with a role.

Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance. Next to each item on the chart, a symbol indicates the type of assignment:

- No icon

  No employees are a member of this role or any of its child roles.

-

-

  Employees that are assigned this role are members of this role.

-

  At least one employee that is assigned this base object, is member of the role or a child role.

To determine usage of a role class

1. Select the role class on the the **Usage** tab.

2. Select a role in the hierarchy.

3. Perform one of the following tasks.

   a. Select a subrole by clicking on the name of the role in the chart.

   b. To move up through the hierarchy, Click the back arrow next to the top of the chart.

   c. Click **Information** to see the assigned employees.

   ⓘ | NOTE: Click **More information** to get more information about the chart and its elements.

Compliance

ⓘ | NOTE: This function is only available when the module Compliance Rules Module is installed.

The **Compliance** tab shows you existing rule violations. If there are rule violations for your selected item, a warning appears.

To view details of a compliance violation

1. Click the **Compliance** tab to view information about the rules that have been violated, the entitlements involved, and the risk index.

2. Mark one of the rule violations in the list to view more detailed information in the detailed content view.

For more information, see Managing Compliance on page 126.

Generating Reports

ⓘ | **NOTE:** This function is only available when the module Report Subscription Module is installed.

Reports that are not created in he Web Portal, are created in the Report Editor and are more comprehensive and complex than reports from the Web Portal. You have other parameters and more data sources can be linked in.

Reports that are created in the Web Portal are simple and can only access value in their own database. Which reports are available to you, is defined in the Manager. An approval workflow for report subscriptions is not required due to this. When you subscribe to a report, you edit the settings it. Subscribed reports are send to you by email.

Viewing, Subscribing and Editing Reports

You will find reports in the Web Portal under **My Actions | Reports** or over **My Settings** menu in the header.

In the **Reports** view you can view and edit subscribed reports or create and subscribe to new reports. The view is divided into two parts.

- Available reports and subscriptions

  This section lists all your subscribed reports. You can identity the reports that you have already subscribed to because they are marked with "(1 subscription)" after the report name. A description of each report is shown in the detailed content view. You can run the following actions on your subscribed reports.

  Table 66: Actions in the detailed content view for reports with marked with "Report Subscription"

Icon	Description
	Subscription settings
	Add employees to this subscription
	Send report now
	Unsubscribe

  You can subscribe to reports with **Subscribe**.

- Owned Reports

  You are responsible for the reports under **Owned Reports** even though you have not subscribed to them.

To subscribe to reports

1. Click on the user name in the header and then **My settings**.

2. Select the **Reports** tab in the **My Settings** view.

3. Select the desired report in **Available reports and subscriptions** and click **Subscribe**.

4. Configure the following settings in **Edit subscription settings** and click Subscribe.

Table 67: Subscription settings

Setting	Description
Subscription	Text box for entering or editing the subscription name.
Schedule	Menu for selecting how often the report is sent. The following options are available: • Monthly report subscriptions • half-yearly report subscriptions • Yearly report subscriptions • Quarterly report subscriptions • Daily report subscriptions • Weekly report subscriptions
Format (e-mail attachment)	Menu for selecting the report format. The report can be sent in the following formats: • CSV • DOCX • HTML • PDF • RTF • TEXT • TIFF • XLS • XLSX • XML • XPS

The following step-by-step instructions take you through how you run the actions on subscribed reports.

To obtain a report immediately

1. Mark the desired report in **Available reports and subscriptions** and click .

2. Select "Daily report subscriptions" under **Schedule** in the **Edit subscription settings** dialog box

3. Save the changes.

   The selected report is sent to your email address.

To end a subscription

1. Mark the desired report in **Available reports and subscriptions** an click 🗑 in the detailed content view.

2. Confirm the prompt with **Yes**.

To edit your report settings

1. Mark the desired report in **Available reports and subscriptions** an click 🖉 in the detailed content view.

2. Make any changes you want in the **Edit subscription settings** dialog box and save them.

To add or remove a subscriber

1. Mark the desired report in **Available reports and subscriptions** and click 👥.

    This opens the **Additional Subscriptions** dialog box. If subscribers have already been added, they are listed in the **Selected** list.

2. Perform one of the following tasks.

    a. Mark the employee you want from the **Available** list.

    b. Select additional columns.

    c. Use the filter function.

    The selected subscription is listed in **Selected**.

3. click **Save**.

    For more information, see Using a Filter on page 23.

Detailed information about this topic

- Creating and Editing Reports in the Web Portal on page 66
- Viewing and Editing your own Reports on page 68

Viewing Reports in the Web Portal

Some views have reports immediately available, generally when the report helps you to make a necessary decision. For example, when you are viewing your file system or SharePoint® resources, you can view reports to help determine ownership. Or when you are performing attestations, you can view current information on the item to which you are attesting.

To run a report

1. Click on the user name in the header and then **My Settings**.

    The view **My Settings** is displayed.

2. Select the **Reports** tab.

    This displays a list of reports.

3. Mark the report you want in the list.

A short description and other details about the selected report is displayed in the detailed context view.

4. Click **View report** in the detailed content view.

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

To generate a report

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

1. Click on the user name in the header and then **My settings**.

2. Select the **Reports** tab in the **My Settings** view.

3. Mark a report and click on **Show report** in the detailed content view.

4. Click **Export this view** in the report view.

   This opens the dialog box **Export this view**. You have several options available.

5. Perform one of the following tasks.

   a. Select either **Export as PDF**.

   b. Select the option **Export as CSV**.

   The report is exported in the respective format.

Auditing Activity and Managing Compliance

Auditing describes how an aspect of a company is assessed. Quality assurance is also plays an important part in auditing. An audit is a systematic, independent and documented examination, which assesses quality-related actions and evaluates them based on the planned requirements and targets. To successfully complete an audit there must be certain features available and specific requirements must be fulfilled.

ⓘ | **NOTE:** You will find the menu **Auditing** in the **Access Governance** main content view.

If you are a manager or compliance officer, you may have access to the **Auditing** menu. The **Auditing** menu gives you a read-only overview of any item for which you are responsible. You can use this to investigate any security issues that arise, or to verify activity. In many cases, you are able to manipulate the view to maximize its value, and export the information to a report. For more information, see Tips for using the Web Portal on page 18.

Detailed information about this topic

- Auditing - Employee Details on page 120
- Auditing - Roles and Entitlements on page 122
- Auditing - Approvals on page 124
- Auditing - Requests on page 124
- Auditing - Attestations on page 125
- Auditing - Rule and Policy Violations on page 125

Auditing - Employee Details

All employees are displayed in a list in the **Auditing | Employee Details** view. Here you can select an employee and view more details. You can select the employee directly from the list or use the Web Portal's filter function. For more information, see Using a Filter on page 23.

After you have selected an employee, the details are displayed on several tabs. You may recognize some of the tabs from the menu **My Responsibilities** in **My Identity**. For more information, see Description of Commonly Used Tabs in Views on page 109.

Table 68: Tab Overview

Tab	Description	Usage
Overview	Displays more details about the employee in a Hyper View.	To view all the information at one glance and navigate quickly to points of interest, click on the linked content in the shapes. For creating reports.
Requests	Lists all the selected employee's requests.	Use the filter function and the advanced search to search selectively.
Approvals	Lists all approvals in the selected period that the select employee was involved in. The list must be filtered on other tabs to see an approval in more detail. • Approvals • Exception approvals • Attestations • Policy violations	Use the filter function and the advanced search to search selectively for approvals. The advance search is only available on the **Approval** tab.
Rule violations	Lists all the selected employee's rule violations.	Use this function to search selectively for rule violations.
Risk	List properties and assignments, which contribute to the calculated risk index.	For viewing risk index functions.
Roles and entitlements	Lists all the selected employee's memberships.	Use the filter function to search selectively for memberships.
Ownerships	Shows ownerships of the selected objects type for this employee.	Shows a more detailed view of ownerships. Use the button in the detailed content view to display more detailed about the selected object.
History	Displays the history of states and comparisons of the selected employee.	You can swap from timeline to table view. Navigate by clicking the mouse within the timeline.

Detailed information about this topic

- Overview on page 110
- Permissions on page 110
- Requests on page 111
- Risk on page 111
- History on page 111
- Employee Approvals on page 122
- Employee Memberships on page 122

Employee Approvals

The **Approvals** tag display all approvals in the selected time period that involved the selected employee. Approval are spread over the following tabs.

- Approvals
- Exception approvals
- Attestations
- Policy violations

ⓘ | **NOTE:** The advance search is only available on the **Approvals** tab.

To search for an approval

1. Open **Auditing | Employee details** and select an employee.
2. Ensure the **Approvals** tag is select on the **Approvals** tag.
3. Use the extended search.

Detailed information about this topic

- How to Search on page 19
- Using a Filter on page 23

Employee Memberships

The **Roles and Entitlement** tab shows all the employee's memberships. You can compare this tab to the **Memberships** tab in the menu **My Responsibilities** in the **My Identity** view.

To view employee memberships in more detail

1. Select the **Roles and Entitlements** tab.
2. Perform one of the following tasks.
   a. Use a filter and then mark the item you want in the result list.
   b. Mark the entry you want in the list.

   This displays details of the selected item in the detailed content view.

Detailed information about this topic

- Using a Filter on page 23
- Auditing - Roles and Entitlements on page 122

Auditing - Roles and Entitlements

On the start page of the menu **Auditing | Roles and Entitlements**, all roles and entitlements are displayed at a glance in the form of large buttons.

You get information about business roles, system entitlements, data accessing, organization structures and other services. For more information, see Managing "My Responsibilities" on page 71.

Table 69: Button Overview

Button		Description	Usage
	Related Applications	Opens an overview listing all applications.	Selects an application.
	Business roles	Opens an overview listing all business roles.	Use the button in the detailed content view to display more detailed about the selected object.
	Cost centers	Opens an overview listing all cost centers.	Specific view of result in which you select an employee responsible for the object.
	Departments	Opens an overview listing all departments.	
	Active Directory®	Opens an overview listing all Active Directory® groups.	
	SharePoint®	Opens an overview listing all SharePoint® groups.	
	Employees	Opens an overview listing all employees	
	Manager Application Roles	Opens an overview listing all application roles.	
	Locations	Opens an overview listing all locations.	
	Resources	Opens an overview listing all resources.	
	System entitlements	Opens an overview listing all system entitlements.	
	System roles	Opens an overview listing all system roles.	

To view all the roles or entitlements for a specific employee

1. Open the **Auditing | Roles and Entitlements** start page and click on the object you want view.

2. Click **Assign** in the overview of the selected object and select an emloyee.

   Any roles and entitlements for the selected employee appear, grouped by object.

3. Perform one of the following tasks.

   a. Use a filter and then mark the item you want in the result list.

   b. Mark the entry you want in the list.

   This displays details of the selected item in the detailed content view.

For more information, see Using a Filter on page 23.

Auditing - Requests

This overview lists all requests that have been created with the selected time period. You can select an employee to view just their requests. To limit the number of list entries you can use the advanced search, the filter function or you can select more columns to display. For more information, see Making and Managing Requests on page 34. Marked requests provide the following information in the detailed content view.

- Details of the requested item
- Status indicates the latest action performed on the request
- General information about the request, including all steps the request has completed, and the next steps
- Details of the recipient and requester
- If there are any rule violations for the request these are displayed with the button **At least one rule was violated**.

To view historical requests

1. Open the menu item **Auditing | Requests** and select an employee using **Assign**.
2. Perform one of the following tasks.

   a. Use a filter and then mark the item you want in the result list.

   b. Use the extended search.

   c. Mark the entry you want in the list.

   This displays details of the selected item in the detailed content view.

   ⓘ | **NOTE:** The **Workflow** tab in the detailed content view shows all changes chronologically in the form of a workflow diagram. Use 🗨 to open a dialog box and view the requester and request number.

Auditing - Approvals

You can use the **Auditing - Approvals** view to see requests involving a particular employee. This view is the same as on the **Auditing - Requests** view. Use the search function to search for a particular request or to filter the results.

To display all historical requests for a specific approver

1. Open the menu **Auditing | Approvals** and select an approver using **Assign**.
2. Perform one of the following tasks.

   a. Use the extended search.

   b. Mark the entry you want in the list.

   This displays details of the selected item in the detailed content view.

   ⓘ | **NOTE:** The **Workflow** tab in the detailed content view shows all changes chronologically in the form of a workflow diagram.

Detailed information about this topic

-
-

Auditing - Attestations

ⓘ **NOTE:** This function is only available if the Attestation Module is installed.

The **Auditing | Attestations** view shows all the attestation cases. The content and type of view vary in presentation depending on the respective company.

To view historical attestation data

1. Open the **Auditing | Attestations** overview page and select an attestor using **Assign**.

2. Enable or disable one or more **Attestation state** options.

3. Perform one of the following tasks.

   a. Use a filter and then mark the item you want in the result list.

   b. Mark the entry you want in the list.

   This displays details of the selected item in the detailed content view.

To notify an attestor about pending attestation cases

ⓘ **NOTE:** You can only contact attestors for attestation cases which have the status **Pending**.

1. Mark an entry with the state **pending** from the list and click **View approvers for pending cases** at the bottom of the detailed content view.

2. Click **Send a mail** next to the employee you want to notify in the **Send a reminder mail** dialog box.

   The email program linked to the Web Designer is displayed and an email template with the attestor's email address is opened.

3. Complete and send the email to the attestor.

   The email program is closed.

Auditing - Rule and Policy Violations

ⓘ **NOTE:** This function is only available if the module Company Policies Module or Compliance Rules Module is installed.

Under the **Rule Violations**, all employees that have violated rules are displayed. The **Auditing - Rule Violations** view shows you all rule violations within a selected time period. Since rule and policy violations are handled similarly, we deal with both topics together in this section. Policy violations granted or denied exceptions or are pending, are shown in the **Policy violations** view.

To view historical rule or policy violation data

1. Perform one of the following tasks.

    a. Open the **Auditing | Rule Violations** menu.

    b. Open the **Auditing | Policy Violations** menu.

2. Select an employee using **Assign**.

3. Perform one of the following tasks.

    a. Use a filter and then mark the item you want in the result list.

    b. Mark the entry you want in the list.

    This displays details of the selected item in the detailed content view.

Managing Compliance

ⓘ **NOTE:** This function is only available if the module Compliance Rules Module, Governance Base Module, Company Policies Module or Attestation Module is installed.

Companies have different requirements that they need for regulating internal and external employee access to company resources. On the one hand, rules are used for locating rule violations and on the other hand, to prevent them. They may also have to demonstrate that they adhere to legislated regulations such as SOX (Sarbanes-Oxley Act). The following demands are made on compliance.

- Rule define to what permissions the employee has or otherwise. For example, a rule could prevent an employee from owning entitlement B if they already have entitlement A.

- Policies are very flexible, and can be defined around anything you are managing with the Manager. For example, a policy could state that only managers in the HR department can have full control over a share on a file share that contains sensitive information.

- Attestations require a manager to verify data to ensure that it is compliant. For example, a manager may need to attest to the Active Directory® groups to which each of his employees belong.

- Each item to which an employee has access can be given a risk value. A risk index can be calculated for employees, 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 - a request will not be processed if it is in violation, unless exception approvals are specifically allowed, and an approver allows it. Rules (if appropriate) and policies are run on a regular schedule, and violations appear on the appropriate employee's Web Portal for handling. Policies may have associated mitigations, which are processes that an employee can do outside of the One Identity Manager solution to reduce the risks posed by the violation. Reports and dashboards give you further insights into your state of compliance. For more information, see What Statistics are Available? on page 100.

The following tasks are compliance activities.

The information you see in the **Compliance** view is highly dependent on your role. If you do not see a menu item that you think you should, contact your system administrator. The following overview shows which view you can see for which user roles.

Table 70: View in the "Compliance" Menu

View	Description	Roles
Resource Access	Lists all existing resources under this menu item. Resources are grouped by resource type.	Compliance & Security Officer
Risk Assessment	Allows you to use calculators in assessing risk. Risk index calculation must be activated by a manager.	Attestation supervisor, policy supervisor, compliance rule supervisor
Attestation policies	Lists attestation policies, and allows editing of existing and creation of new policies.	Compliance officer, attestation supervisor
Policy violations	Provides reports on objects which violate policies.	Framework administrator, policy supervisor and rule exception approver
Compliance Frameworks	Provided details about the compliance frameworks in your environment.	Compliance framework administrator
Rule violations	Provides reports on employees who violate policies.	Framework administrator, rule supervisor and rule exception approver
High Risk Overview	Provides an overview of critical objects. The overview is divided into several parts.	Compliance & Security Officer
Rule analysis	Identifies employees who are in violation of rules related to SAP functions. You must configure SAP authorizations for testing. For more detailed information about SAP® R/3® Compliance Add-on, see the Dell One Identity Manager Identity Management Base Module Administration Guide. ⓘ NOTE: SAP function calculation must be activated by an manager.	Compliance framework administrator
Function analysis	Specifies employees whose access to high risk SAP function violates the rules. ⓘ NOTE: functions calculation must be activated by an manager.SAP	Rule supervisor

Modifying Risk Calculators

Risk assessment is an important part of compliance. For example, high risk rule violations are more likely to require mitigations, or have fewer exception approvers. In the One Identity Manager, risk data is gathered from a variety of sources, and then calculations are performed to produce risk indexes. Every item within the One Identity Manager can be assigned a risk value. If you own resources, you maybe able to modify their risk values in the Master Data. For more information, see Editing Master Data of Business Roles, System Roles and other Services on page 82.

> ⓘ | **NOTE:** You will find the menu **Administration** in the **Governance Administration** main content view.

In the **Risk Assessment** view, you can modify the risk index functions that are used to calculate these indexes. Risk indexes are calculated for employees, user accounts, system roles, IT Shop structures, organizations and business roles.

There are four calculation types that can be used. Choose the one that best fits the desired impact on risk for the risk index function you are modifying.

Table 71: Calculation Types

Calculation type	Description
Maximum (weighted)	The highest value from all relevant risk indexes is calculated, weighted and taken as basis for the next calculation.
Maximum (normalized)	The highest value from all relevant risk indexes is calculated, weighted with the normalized weighting factor and taken as basis for the next calculation.
Increment	The risk index of Table column (target) is incremented by a fixed value. This value is specified in **Weighting/Change value**.
Decrement	The risk index of Table column (target) is decremented by a fixed value. This value is specified in **Weighting/Change value**.
Average(weighted)	The average of all relevant risk indexes is calculated, weighted and taken as basis for the next calculation.
Average(normalized)	The average of all relevant risk indexes is calculated with the normalized weighting factor and taken as basis for the next calculation.
Reduction	Used when calculating the reduced risk index for rules, SAP functions, company policies and attestation policies. You cannot add custom functions with this calculation type!

You can assign a weight to the calculation, which determines how much the result of a particular function affects the overall risk index. You can view high risk objects in the view **High Risk Overview**. For more information, see What Statistics are Available? on page 100.

To modify a risk index function

1. Open the menu **Administration | Risk Assessment** and select the risk index function.

2. Click 📝 and select the calculation type in the **Attestation assignment** dialog box.

3. Use the slider to set a value between 0 and 1 on the **Weighting/Change value** scale.

To disable or enable a risk index function

1. Open the menu **Administration | Risk Assessment** and select the risk index function.

2. Click 🖉 and perform one of the following actions:

   a. Check the **Disabled** box if you do not want to use the risk index function.

   b. Uncheck the **Disabled** box to use the risk index function again.

3. click **Save**.

Performing Attestations

Managers or others responsible for compliance can use attestation policies to run the following tasks.

- Authorize access
- Set up permissions

Attestations start with attestation policies. You use these policies to specify which objects are designated for attestation and when and how often they are run.

You can get a high level overview of the attestations in your organization in the Attestation dashboard. For more information, see What Statistics are Available? on page 100.

ⓘ **NOTE:** To open **Administration | Attestation Policies** menu, you must select the main menu item **Governance Administration**. For more information, see Navigating around the Web Portal on page 12.

The following activities are involved in the attestation process:

- Working with Attestation Policies on page 129
- Selecting Object Link Types on page 136
- Approving and Denying Attestations on page 136
- Viewing Completed Attestations on page 141

Working with Attestation Policies

If you are responsible for attestation policies, you can work with the **Attestation Policies** menu. The following functionality can be edited in attestation policies.

- Setting up a schedule after the attestation case is generated.
- Select an employee to be responsible for granting or denying approval of attestation cases.
- Enable/disable the setting used by the system to automatically close redundant attestation cases.

Apart from editing attestation policies, you can also create conditions and edit them. This function makes it possible for you to view all objects adhering to a certain condition. For more information, see Approving and Denying Attestations on page 136.

You cannot edit all the properties in existing policies. This depends on your access permissions. All attestation policies with the following information are displayed various on tabs under the **Attestation Policy** menu.

Table 72: Attestation policy - "Attestation Policy Settings"

Column	Description
Attestation policy	Name of the attestation policy.
Attestation procedure	Name of the attestation procedure.
Compliance framework	Compliance frameworks are used for classifying attestation policies, compliance rules and company policies according to regulatory requirements.
Calculation schedule	Schedule used to generate new attestation cases.
Owner	Employee that created the attestation policy.
Actions	Several actions are available in this column. For example, you can edit, copy or delete.

ⓘ | **NOTE:** The option **Show disabled policies** must be set to view this policies.

Table 73: Attestation policy - "Attestation Policy Runs"

Column	Description
Attestation policy	Shows attestation policies that have already been run.
Run started	Start date of the attestation run.
Due date	Date on which the attestation run should end.
Progress so far	Shows the progress of already generated attestation cases of an attestation policy. Progress is shown in percent (only integer values) and with a colored bar. Progress under 70%, red bar. Progress above 90%, green bar. Progress between 70% and 80%, orange bar.

Once you have selected an attestation policy, you can view other details about it. These details are explained in the following table.

Table 74: Description of the detailed content view

Content module / tab	Description
Data	This content module is on the **Details** tab. You will find information about the attestation run, expiry date and progress up to now next to the name of the attestation policy.
Attestation details	This content module you can view current pending, completed and delegated attestations. Another value is the total value of all existing attestation cases. There are more details about attestation cases with escalation and about speed of attestations.
Attestation forecast	Details such as the predicted progress on the due date and predicted end date of the run are part of the attestation forecast. More predictions about estimated delays, when attestation would expire under the currently given conditions. Apart from this, attestation is already graded into categories **Good**, **Mediocre** and **Bad**.

Content module / tab	Description
Attestors	Information about opened and closed attestation cases and the attestors involved are displayed for the selected attestation run on the **Attestors** tab. You can send reminders to the Compliance & Security Officer and the attestation policy owner but only if there are still pending attestation cases for this attestation policy. You can also renew the attestation, giving a reason.

Sending Reminders to Attestors

To send a reminder to an attestor

1. Open the menu **Administration | Attestation policies** and select an attestation policy on the **Attestation Policy Runs** tab.

    ⓘ **NOTE:** For the **Min. category**, you can choose between **Good**, **Mediocre** and **Bad** to limit the attestation policies shown.

2. Enable the attestor you want on the **Attestor** tab in the detailed content view.

    ⓘ **NOTE:** You can multi-select approvers or you can select all attestors by setting the last check box in the list.

3. Click **Send reminder**.

Editing Attestation Policies

To edit an attestation policy

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

2. Mark the desired attestation policy and click on 📝 in the **Actions** column.

    ⓘ **NOTE:** The system contains default attestation policies. These policies can only be edited to a limited degree. Only **Approval policies**, **Calculation schedule**, **Time required** and the option **Close obsolete tasks automatically** could be edited until now. If you want to make changes to a default attestation policy, create a copy and edit the copy.

    ⓘ **NOTE:** If the option **Close obsolete tasks automatically** is set, you cannot hide processed attestation cases which are beyond the deadline.

3. Edit the policy as required on the **Master Data** tab.

    For more information, see Creating New Attestation Policies on page 135. You can also add new conditions, change or delete existing ones. You permissions determined which data you may edit. For more information, see Adding or Deleting a Policy Condition on page 132.

4. click **Save**.

Adding or Deleting a Policy Condition

To add a condition to a policy

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

2. Edit the desired attestation policy.

   For more information, see Editing Attestation Policies on page 131.

3. Click in the **Object selection** view on the **Master data** tab.

4. Select the option you want in the **Condition type** menu in the **Edit condition** dialog box.

   ⓘ | **NOTE:** The options available in **Condition type** depend on which attestation procedure is set for the attestation policy to be edited.

   The following options are available.

   Table 75: Available Condition Types

Condition Type	Description
All roles / cost centers	Lists all company structures.
	Multi-select is possible. Selected parameters are listed in the detailed content view and can be canceled again there. Or you cancel the selection in list again.
Attestation by attestation status / Roles by assignment type	Lists attestations by status or role assignment type as other parameter.
	Multi-select is possible. Selected parameters are listed in the detailed content view and can be canceled again there. Or you cancel the selection in list again.
Specific roles / cost centers	List certain roles for the company structure,
	You can toggle between tree view and list view using and . Multi-select is possible. Selected roles are listed in the detailed content view and can be reselected there. Or you cancel the selection in list again.
Business roles / Application roles / Cost centers with matching names	Displays the **Name** text box.
	Enter a name for the company structure.
New or not attested for x days	Displays the **Count** text box.
	You can enter the count.
Roles with specific owners / user accounts with specific people / Roles with any owner	Lists certain employees for the company structure.
	Additional columns can be shown and the filter function applied. Multi-select is possible. Selected employees are listed in the detailed content view and can be canceled again there. Or you cancel the selection in list again.

Condition Type	Description
Roles with specific role classes	Lists specific role classes.
	Multi-select is possible. Selected role classes are listed in the detailed content view and can be canceled again there. Or you cancel the selection in list again.
Roles with defined risk index	Display a scale of 0 to 1 for the risk index and two slide rulers.
	Specify a beginning and an end value within the scale.
Roles with owners in departments	Lists departments which have owners.
	Multi-select is possible. Selected role classes are listed in the detailed content view and can be canceled again there. Or you cancel the selection in list again.

5. Save the changes.

To remove a condition from a policy

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

2. Edit the desired attestation policy.

   For more information, see Working with Attestation Policies.

3. Mark the condition you want in the **Object selection** view on the **Master data** tab and click 🗎 in the **Action** column.

   This deletes the condition.

Adding a Condition for Special Data Queries

To add a condition, which includes objects whose names contain a specific string

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

2. Perform one of the following tasks.

   a. Create a new attestation policy.

      For more information, see Creating New Attestation Policies on page 135.

   b. Edit the desired attestation policy.

      For more information, see Editing Attestation Policies on page 131.

3. Perform one of the following tasks.

   a. Add a new condition.

      For more information, see Adding or Deleting a Policy Condition on page 132.

   b. Edit an existing condition.

      For more information, see Editing Policy Conditions on page 134.

4. Select the option **...with matching names** in the **Edit condition** dialog box in **Condition type**.

5. Enter part of the name to filter the object by in **Name** and click **OK**.

Editing Policy Conditions

To edit a policy condition

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

2. Edit the desired attestation policy.

   For more information, see Editing Attestation Policies on page 131.

3. Mark the condition you want in the **Object selection** view on the **Master data** tab and click 🖊 in the **Action** column.

4. Make your changes in the **Edit condition** dialog box and save them by clicking **OK**.

   For more information, see Adding or Deleting a Policy Condition on page 132.

Using a Filter to Display Attestation Objects

To display all objects for attestation after applying a filter for valid conditions

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

2. Edit the desired attestation policy.

   For more information, see Editing Attestation Policies on page 131.

3. Perform one of the following tasks.

   a. Mark your condition on the **Master Data** tab in the **Object selection** pane and click on the linked number in the **Objects** column.

   b. Click the linked number under the list of conditions.

   All objects which meet the condition/s are displayed in a dialog box.

Updating Object Selection in the View

To update the object selection list

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

2. Edit the desired attestation policy.

   For more information, see Editing Attestation Policies on page 131.

3. Click 🔄 in the **Object selection** view on the **Master data** tab.

   This reloads the object selection. New conditions, which may also be added to the , are also shown.Manager For more information, see the Dell One Identity Manager Attestation Administration Guide.

Creating New Attestation Policies

To create a new attestation policy

1. Open the **Administration | Attestation Policies** menu and select the **Attestation Policy Settings** tab.

2. Click **New attestation policy** and enter the following attestation policy data.

   ⓘ | **NOTE:** The attestation procedure you select when you create a new attestation policy is important. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The available options are modified to match the attestation procedure.

Table 76: General Master Data for Attestation Policies

Property	Description
Attestation policy	Text box for entering a unique name for the attestation policy.
Attestation procedure	Selecting the appropriate attestation procedure using **Assign**.
Approval policies	Selection of the appropriate approval policies using **Assign**.
Calculation schedule	Selection of the appropriate calculation schedules using **Assign**.
Time required (days)	Select of the number of days which specifies the deadline for making an attestation procedure approval decision.
Compliance Frameworks	Assignment of an attestation policy to a compliance framework using **Assign**.
Disabled	If this option is set, the new attestation is disabled. This option is not set by default.
Close obsolete tasks automatically	If this option is set, obsolete cases are automatically closed. This option is set by default.
Description	Text box for entering additional information and conditions for the attestation policy.

3. Click **Create**.

New Attestation Policy Based on Existing Policies

To create a new attestation policy based on an existing policy

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

2. Mark the basis policy and click 📋

3. Confirm the alert box with **Yes** and edit the policy as you wish on the **Master data** tab.

   For more information, see Creating New Attestation Policies on page 135.

4. Enable a filter criteria in the **Object selection** view, if necessary, and click **Save.**.

Selecting Object Link Types

Before you save data or changes for attestation policies, you can set the link type for selecting the object. Set this in the **Attestation procedure** when you add or edit a new attestation policy. The following link types are available.

Table 77: Link Types

Link Type	Description	Example
All conditions must be fulfilled:	New attestation cases are added for all objects fulfilling all of the conditions the next time the attestation policy is executed. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this link type generates a intersecting set of all the individual conditions of the selected objects.	Example: For the attestation policy of type "Membership in organizations" there are the condition "Departments with matching names" and "Attestation by attestation status". If this link type is set, the sum of the results for both conditions is displayed in addition to the results for each condition separately.
At least one condition must be fulfilled:	New attestation cases are added for all objects fulfilling at least one of the conditions the next time the attestation policy is executed. Use of this link type generates a superset of all the individual conditions of the selected objects.	Several conditions apply to the attestation policy mentioned above. During the attestation case, the superset of attestation objects is displayed as the sum of objects found because this link type requires at least condition to be met.

To select object link types

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

2. Perform one of the following tasks.

    a. Create a new attestation policy.

       For more information, see Creating New Attestation Policies on page 135.

    b. Edit the desired attestation policy.

       For more information, see Editing Attestation Policies on page 131.

3. Perform one of the following tasks.

    a. Assign an attestation procedure to the attestation policy using **Assign** on the **Master Data** tab.

    b. Assign a different attestation procedure to the attestation policy using **Change** on the **Master Data** tab.

4. Save the changes.

Approving and Denying Attestations

Attestations are a way of verifying that security and compliance measures are being met. For example, having a manager attest to the groups his employees belong to provides accountability if security breaches are found. Attestation policies define what and whom to attest.

Attestation policies are run on a schedule, and generate attestation cases. These appear on the **My Actions** menu. The amount of time you are give to close an attestation case is configured as part of the attestation policy.

ⓘ **NOTE:** The main menu **My Identity** must be selected in order to select the menu **My Actions**. For more information, see Navigating around the Web Portal on page 12.

As an attestor, you must be able to verify your attestations. Verifying attestations requires reading reports or manually checking object that are attested. If you are not ready to make a decision, you may be able to:

- Generate a report that provides detailed information about the object which you are attesting
- Request more information, add attestors, or delegate the attestation.

To generate a report to provide you with information for the attestation case

1. Open the menu **My Actions | Pending Attestations** and select one the following actions.

   a. Click on an object type.

      This displays all the matching attestation policies for this object type.

   b. Click **View attestation policies**.

      This displays all attestation policies.

2. Mark the desired case.

   This displays details of the selected case in the detailed content view.

   ⓘ **NOTE:** Not all attestation cases have reports available.

3. Click **Export this view** in the selected policy's view.

   This opens the dialog box **Export this view**. For more information, see Exporting a View on page 30.

To view new attestation cases

All the attestation policy attestation cases are displayed. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before. These cases are marked with "Yes" in the column, **New**.

ⓘ **NOTE:** You can add the column **Not approved before** to your table view by showing additional columns. This provides the same information as in the **New** column, which is shown in the table by default.

1. Open the menu **My Actions | Pending Attestations** and select one the following actions.

   a. Click on an object type.

      This displays all the matching attestation policies for this object type.

   b. Click **View attestation policies**.

      This displays all attestation policies.

2. Mark the new attestation case and view more details about the case in the content view.

To approve or deny an attestation case

1. Open the menu **My Actions | Pending Attestations** and select one the following actions.

   a. Click on an object type.

      This displays all the matching attestation policies for this object type.

   b. Click **View attestation policies**.

      This displays all attestation policies.

2. Mark the desired case in the Pending Attestations view.

3. Perform one of the following tasks.

    a. Click ☑ to grant approval.

    b. Click ☒ to deny approval.

4. Repeat step 3 if necessary and click **Next**.

5. Perform one of the following tasks.

    a. Enter a reason to justify your decision in the text box.

    b. Select a predefined reason in **Standard reasons**.

    ⓘ | **NOTE:** You can optionally select a predefined text from **Standard reasons** for all cases still to be approved. Standard reasons are displayed in the approval history and in the case details. For more detailed information about default reasons, see the Dell One Identity Manager Attestation Administration Guide.

6. Click **Save approvals**.

    ⓘ | **NOTE:** Some attestation cases that still need to be approved, require Multi-factor authentication. After your approval decision has been saved, you will prompted to enter a security code. For more information, see Requesting Products requiring Multi-Factor Authentication on page 43.

    ⓘ | **NOTE:** If you want to grant or deny approval to the entire list of attestation cases, you can set the option **Approve all** or **Deny all** before clicking **Save decision**.

To view an attestation object

1. Open the menu **My Actions | Pending Attestations** and select one the following actions.

    a. Click on an object type.

       This displays all the matching attestation policies for this object type.

    b. Click **View attestation policies**.

       This displays all attestation policies.

2. Mark the desired case.

   This displays details of the selected case in the detailed content view.

3. Select**Go to attested object** in the **Actions** menu.

   This opens a view for the selected object.

To view attestation for a specific object type

1. Open **My Actions | Pending Attestations** and click on an object type.

   This displays all the matching attestation policies for this object type.

    ⓘ | **NOTE:** How you proceed, depends on the object type you select.

2. Perform one of the following tasks.

   a. Proceed as follows, if you selected the object type **Cost center**.

      A list of your selected object types appears in the view.

      - Select your cost center.

        This displays the pending attestations for the selected cost center with the tabs **Object attestation** and **All attestation cases**.

   b. Proceeds as follows, if you select the object types **People** or **Business Roles**.

      A list of your selected object types appears in the view.

      - Select the object type for which you want to view the attestation, for example, "employee".

        In the **Pending Attestations** view you can see the tabs **Memberships** and **All attestation cases**.

3. Select the tab you want to view.

   This displays a list of attestation cases for the selected tab.

4. Mark the attestation you want to view in detail.

   In the detailed content view you see several tabs containing detailed information about attestation.

To send a reminder to an attestor

1. Open the menu **My Actions | Pending Attestations** and select one the following actions.

   a. Click on an object type.

      This displays all the matching attestation policies for this object type.

   b. Click **View attestation policies**.

      This displays all attestation policies.

1. Mark the desired case.

   This displays details of the selected case in the detailed content view.

2. Select the action **Send a reminder mail**.

   This opens the dialog box **Send a reminder mail**, with a list of employees who may approve the attestation case.

3. Mark the employee you to remind and click **Send a mail**.

   The email program linked to the Web Designer is displayed and an email template with the attestor's email address is opened.

4. Complete the message and the email to the attestor.

   The email program is closed.

To view employees with approval authorization for an attestation case

1. Open the menu **My Actions | Pending Attestations** and select one the following actions.

   a. Click on an object type.

      This displays all the matching attestation policies for this object type.

b. Click **View attestation policies**.

This displays all attestation policies.

2. Mark the desired case.

This displays details of the selected case in the detailed content view.

3. Select the **Workflow** tab.

This displays the current authorized approvers and approval authorized employees who have already made approvals.

To view previous attestation cases for an object

1. Open the menu **My Actions | Pending Attestations** and select one the following actions.

a. Click on an object type.

This displays all the matching attestation policies for this object type.

b. Click **View attestation policies**.

This displays all attestation policies.

2. Mark the desired case.

This displays details of the selected case in the detailed content view.

3. Select the **History** tab.

This displays a list of the attestation cases that have already taken place for the selected object. You can get more information about each attestation case.

Detailed information about this topic

- Auditing - Attestations on page 125

Editing Attestation with the Chief Approval Team

If the are attestations pending and the approver responsible is not available for an extended period or has no access to Web Portal, the fallback approver or member of the chief approval team must make an approval decision. For more detailed information about the chief approval team, see the Dell One Identity Manager Attestation Administration Guide.

ⓘ **NOTE:** You only see the menu item **Attestation escalation** if you are a fallback approver or member of the chief approval team.

To view escalated attestations

- Open **My Actions | Attestation Escalation Approval**.

This displays escalated attestations.

Escalated attestations are handled in the same way as pending attestations. For more information, see Approving and Denying Attestations on page 136.

ⓘ **IMPORTANT:** The four-eye rule can be broken like this because chief approval team members can make approval decisions about Attestation cases at any time!

Viewing Completed Attestations

You can view attestation cases you approved or denied under the menu item **Attestation History** in menu **My Action History**. If you are an auditor or manager, you may be able to view attestations performed by other employees. For more information, see My Action History on page 107 and Auditing - Attestations on page 125.

ⓘ **NOTE:** The main menu **My Identity** must be selected in order to select the menu **Attestation History**. For more information, see Navigating around the Web Portal on page 12.

Viewing Your own Attestation Policies

ⓘ **NOTE:** If a Compliance & Security Officer has assigned ownership of an attestation policy to you, you can view this policy in the main content **Governance Administration** in the menu **Administration | Attestation Policies**.

To view your own attestation policies

1. Open the menu **Administration | Attestation policies** and select the tab **Manage attestation policies**.

   ⓘ **NOTE:** Of the attestation policies you want to view, you are only shown those with attestation runs. If there are no attestation runs, the attestation policies are not listed.

2. Mark your attestation policy.

   More information about the policy is displayed in the detailed content view. For more information, see Working with Attestation Policies on page 129.

   ⓘ **NOTE:** If you have no other permissions, you can only view your attestation policies. You cannot edit them.

Viewing Compliance Frameworks

ⓘ **NOTE:** This function is only available if at least one of the modules Governance Base Module, Attestation Module, Compliance Rules Module or Company Policies Module is installed.

Compliance frameworks group together various policies, rules, and attestations to correspond with regulatory requirements. Compliance frameworks are set up by an administrator, but can be viewed in the Web Portal.

This is required, for example, of you must comply to a certain framework. It is useful to know, which rules, policies and attestation policies are connected with the framework.

ⓘ **NOTE:** The main menu **Access Governance** must be selected in order to select the menu **Compliance**. For more information, see Navigating around the Web Portal on page 12.

To view a compliance framework

- Open the **Compliance | Compliance Frameworks** menu and select a framework.

  A Hyper View of the framework appears, with a shape for the associated rules, policies and attestation policies. For more information, see Tips for using the Web Portal on page 18.

Managing Rule and Policy Violations

Not adhering to rules and policies to leads to violations. Violation can occur as part of a workflow (for example, when an employee requests a policy, which violates a rule) or as part of scheduled testing. You can take the following action, depending on your role.

- Editing Pending Violations
- Displaying Rule and Policy Violations
- Identifying High Risk SAP Users (Rule Analysis and Critical Function Analysis)

Editing Pending Violations

Some rule and policy violations can be approved as an exception. Violations that you can approve or deny, are displayed in the **My Actions** menu. The following information is displayed in the corresponding menu.

Table 78: Managing Rule and Policy Violations

Display	Description
Employee	Employee who caused the rule violation.
Violating object	Object, which caused the violation.
Rule	Violated rule.
Policy	Violated policy.
Approval state/Status	The status of the approval. Following states are possible. • Open • Exception granted • Exception denied
Approver	Employee who has denied or granted exception approval.
Approval date	Date of the approval decision.
Risk index (calculated)	Shows the calculated risk index.
Risk index (reduced)	Shows the risk index reduced by the mitigating control.
Reason	Shows the manually entered reason added with the exception approval.
Standard reason	Displays a standard reason if one exist and this option was selected.
Valid until	The exception is only valid until this date.

If you are an auditor or an approver, you can obtain more information about exception approvals from the **Auditing** menu. For more information, see Auditing - Rule and Policy Violations on page 125.

To grant or deny exception approvals

1. Perform one of the following tasks.

    a. Open the menu **My Actions | Pending Rule Violations** for rule exception.

    b. Open the menu **My Actions | Pending Policy Violations** for policy exceptions.

2. Use the filter function in the **Approval state** column and set the option **Decision pending**.

    Only the rule or policy violations of the selected type are displayed. For more information, see Using a Filter on page 23.

3. Mark the rule or policy violation you want in the list.

    This displays details of the violation in the detailed content view and you can carry out various actions. How you continue, depends on the view you find yourself in.

4. Perform one of the following tasks.

    a. Approve the violation by clicking on ☑ and click **Next**.

    b. Deny the violation by clicking on ☒ and click **Next**.

    Your selected is highlighted.

5. To edit a rule or policy violation:

    a. Mark the violation and edit the available settings in the detailed context view.

    b. Click **Assign** and select an exception.

        Assigns the selected mitigating control to the case.

        ⓘ | **NOTE:** If you want to change a mitigating control, click **Change**.

    c. Click **Next** in the detailed context view.

        This displays the **Approval exceptions** view.

    d. Perform one of the following tasks.

        • Enter an reason for your approval decision.

        • Select a predefined reason.

        ⓘ | **NOTE:** You can optionally select a predefined text from **Standard reasons** or using the link **Assign** for all cases still to be approved. Standard reasons are displayed in the approval history and in the case details. For more information about default reasons, see the Dell One Identity Manager Compliance Rules Administration Guide or the Dell One Identity Manager Company Policies Administration Guide.

        ⓘ | **NOTE:** If you are editing several rule or policy violations at the same time, you can enter a reason for each one individually.

    c. Click **Save approvals**.

        Your approval decision is saved and the rule or policy violation's status changes accordingly.

To view the history of your exception decisions

1. Perform one of the following tasks.

    a. Open the menu **My Action History | Rule Violation History** if it is a rule exception.

    b. Open the menu **My Action History | Policy Violation History** if it is a policy exception.

2. Use the filter function in the **Approval state** column and set the option **Exception granted** or **Exception denied**.

   Only historical rule or policy violations of the selected type are displayed. For more information, see Using a Filter on page 23.

3. Select the rule or policy violation in the list.

   You can view more information in the detailed content view.

   ⓘ | **NOTE:** For more information about rule or policy violation approval decisions, see **To grant or deny exception approvals**.

Displaying Rule and Policy Violations

Certain roles require you to find policy violations within their own system. This information can help fill holes in security or compliance politic and help develop attestation policies or violation mitigation. Mitigation comprises of processes existing outside the One Identity Manager solution and which reduce the risk of violation. For more information, see Managing Compliance on page 126.

You can generate reports, which exactly describe the rule or policy violations. 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 many risk factors arising from violations into account and represent the risk as a value between 0 (no risk) and 1 (high risk). The following three views are available which can be reached through the listed links in a table in the corresponding columns.

- Compliance Framework Overview

  Shows all policies or rules within the framework, which were violated and the number of exceptions granted and denied.

- Compliance Rule or Policy Group Overview

  Show the groups of rules or policies, which were violated and the number of exceptions granted and denied.

- Compliance Rile and Policy Overview

  Shows violations of the selected rule or policy grouped by:

  Violations still pending an approval decision

  Violations without exception

  - Violations with exception approval

ⓘ | **NOTE:** You can only see the menu item **Policy violations** or **Rule violations** if you have the Compliance & Security Officer's or Auditor's application role.

Depending on which application is assigned to you, the following options in your rule violation view are visible to you:

- By framework
- By department

- By rule
- By application role
- All compliance rules

ⓘ | **NOTE:** If you only have one application role, you will not see any other options. The option corresponding to the application in this case is preset and must not be enabled by you.

To view rule violations

1. Select **Compliance | Rule violations** and set the display options to get a better overview.
2. Perform one of the following tasks.

   a. Select a framework.

   b. Select a rule.

   Depending on you role assignments, you can generate a report using the **Report** button.

Depending on which application is assigned to you, the following options in your rule violation view are visible to you:

- Framework administrator
- All Policies

To view rule violations

1. Select **Compliance | Policy violations** and set the display options to get a better overview.
2. Perform one of the following tasks.

   a. Select a framework.

   b. Select a policy.

   Depending on you role assignments, you can generate a report using the **Report** button.

Identifying High Risk SAP Users (Rule Analysis and Critical Function Analysis)

Users who have access to certain SAP functions, and who have violated compliance rules can pose a significant security threat. You should analyze these users to determine if action should be taken. Two views in the Web Portal help you with this task.

- Rule analysis

  Shows you compliance rules that contain SAP functions, and identifies any employees who violate the rule. You can analyze the rule violation to determine the cause.

- Function analysis

  Shows you employees with critical SAP functions, which violate compliance rules. For each employee, you can determine what SAP function is involved in the violation, and the rules that caused the violation. You can use the significance rating to prioritize your actions. If a rule with a significance rating is violated by a SAP function with a significance rating it must be handled promptly.

To obtain information about SAP user accounts involved in a rule violation

1. Select **Compliance | Rule Analysis**.

   A list of all rules that include SAP function appears.

2. Click **Select** in the desired entry, to view user accounts and employees who have violated compliance rules.

   You can determine which rules have violations by using the Critical Function Analysis.

   For any employee who has violated the rule, you can analyze the violation by role or ability.

3. Click **By role** to expand details about roles and profiles for the rule violation.

4. Click **Back** to return to the list of employees.

5. Click **By ability** to expand details of SAP functions and transactions.

To identify employees who violate compliance rules with critical SAP functions

1. Select **Compliance | Function Analysis**.

   A list of employees with critical SAP functions appears.

2. Click **Select** to expand details of SAP functions and rule violations for the selected employee.

Administration

The **Administration** section, deals with the administrative functionality in the Web Portal. You will find this section on the **Access Governance** main content page assuming you have sufficient access permissions.

Detailed information about this topic

Target System Administrators

You will find target system administrator responsibilities on the **Governance Administration** page.

- Add a new owner role and assign a product owner to an Active Directory® group if you are target system administrator. You can also edit the requestability of a Active Directory® group.

- Change the properties of the entitlement. For more information, see Editing Master Data of Business Roles, System Roles and other Services on page 82.

To assign a new product owner to an Active Directory® groups

ⓘ | **NOTE:** This function is only available when the module Active Directory Module is installed.

1. Open the menu **Target systems | System entitlements** and select your Active Directory® group.

    ⓘ | **NOTE:** Before you can assign a new product owner, you must add a new owner role for this employee.

2. Select the tab **Owners** and click **Create new owner role**.

3. Enter a name for the new owner role and a reason for creating it.

    ⓘ | **NOTE:** After adding the new owner role, assign a product owner to it.

4. Select a product owner using **Assign** and the new owner role with **Product owners**.

    ⓘ | **NOTE:** If the entry **Without owner in AD** was selected in the **Product owner** dialog box, you cannot select a product owner.

To assign an attestor to a Active Directory® group

1. Open the menu **Target system | System entitlements** and select your Active Directory® group.

   ⓘ | **NOTE:** Before you can assign a new attestor, you must add a new application role.

2. Select the tab **Attestor** and click **Create new attestor application role**.

3. Enter a name for the new application role and a reason for creating it.

   ⓘ | **NOTE:** After adding the new application role, assign an attestor to it.

4. Select the new application role over **Assign** and the new application role with **Attestor**.

Managing Business Roles

As a business role administrator, you can view every role in the **Governance Administration** main content and edit them. Deleted roles can be restored.

To view business roles

1. Open the menu **Identity Management | Business Roles**.

   By default, all roles are listed with their names, managers and roles classes. Use the **Additional Columns** link to display more detailed about the business classes.

2. Mark the desired role.

   To search for the role you want, you have the usual help available such as a filter function, filter wizard and the search function. For more information, see Tips for using the Web Portal on page 18.

To edit a role

1. Select your role and click **Edit** in the main content view.

   This open a view for the selected role with several tabs, which you will recognize from the **My Responsibilities | Business Roles** menu.

2. Perform one of the following tasks.

   a. Edit the master data.

      For more information, see Editing Master Data of Business Roles, System Roles and other Services on page 82.

   b. Request or delete memberships.

      For more information, see Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services on page 81.

To restore a deleted role

1. Select the role you want to restore and click in the main view on **Restore a deleted role**.

   A dialog box appears. The view **Select deleted role** is enabled and lists all the deleted objects.

   ⓘ | **NOTE:** You can set a date in order to limit your search for deleted roles.

2. Select the desired role and click **Next**.

   Multi-select is possible. The view **Test** appears and lists the actions that will be run on restore.

3. You can deselect individual actions if you do not want to run them all. Click **Next**.

4. Close the dialog box.

Detailed information about this topic

- Administration of Organizations on page 149

Administration of Organizations

As administrator, you can view and edit all the organization roles on the main content page, **Governance Administration**. Deleted roles can be restored. Organizations are divided into cost centers, departments and locations.

To select an organization

1. Open the menu **Identity Management | Organization**.

   This opens the **Organization** view.

2. Select the desired organization type.

   This lists all the roles belonging to the selected organization type. Use the **Additional columns** link to display more details about the organization type.

3. Marked the required role.

   To search for the role you want, you have the usual help available such as a filter function, filter wizard and the search function. For more information, see Tips for using the Web Portal on page 18.

To edit a role

1. Select your role and click **Edit** in the main content view.

   This open a view for the selected role with several tabs, which you will recognize from the **My Responsibilities | Business Roles** menu.

2. Perform one of the following tasks.

   a. Edit the master data.

      For more information, see Editing Master Data of Business Roles, System Roles and other Services on page 82.

   b. Request or delete memberships.

      For more information, see Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services on page 81.

To restore a deleted role

1. Select the role you want to restore and click in the main view on **Restore a deleted role**.

   This opens a dialog box. The view **Select deleted role** is enabled and lists all the deleted objects.

   ⓘ | **NOTE:** You can also select **Select deleted role** before you select the organization type.

   ⓘ | **NOTE:** You can set a date in order to limit your search for deleted roles.

2. Select the desired role and click **Next**.

Multi-select is possible. The view **Verify** appears and lists the actions that will be run on restore.

3. You can deselect individual actions if you do not want to run them all. Click **Next**.

4. Close the dialog box.

Detailed information about this topic

- Managing Business Roles on page 148

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.quest.com.

Contacting Dell

For sales or other inquiries, visit http://quest.com/company/contact-us.aspx or call +1 949 754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.quest.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. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to http://quest.com/trials.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer

Index