

Dell™ One Identity Manager 7.0

Web Portal User Guide



© 2015 Dell Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Dell Software Inc.

The information in this document is provided in connection with Dell Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell Software products. EXCEPT AS SET FORTH IN DELL SOFTWARE'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Dell Software Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (www.software.dell.com) for regional and international office information.

Patents

This product is protected by U.S. Patent # 8,639,827 and # 8,601,539. Additional patents pending.


Trademarks


Dell™, the Dell logo, and Dell™ One Identity Manager, Dell™ Dell™ Active Roles, Dell™ One Identity Password Manager, and Dell™ One Identity Cloud Access Manager are trademarks of Dell Inc. and/or its affiliates.

Microsoft, Outlook, Active Directory, SharePoint, SQL Server, Forefront, Internet Explorer, Visual Studio, Windows Server, Windows PowerShell, Windows Vista and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. SAP, SAP R/3, SAP NetWeaver Application Server, and BAPI are trademarks or registered trademarks of SAP AG (or an SAP affiliate company) in Germany and other countries. IBM, Lotus Notes and LotusScript are registered trademarks of International Business Machines Corporation. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Oracle and Java are registered trademarks of Oracle and/or its affiliates. UNIX is a registered trademark of The Open Group. Mono, and SUSE are registered trademarks of Novell, Inc. Apache and Apache HTTP Server are trademarks of The Apache Software Foundation. Firefox is a registered trademark of the Mozilla Foundation. Safari is a registered trademark of Apple Inc. Chrome and Google are trademarks or registered trademarks of Google Inc., used with permission.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

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

One Identity Manager Web Portal User Guide
Updated - July 2015
Software Version - 7.0

Contents

- Getting Started with the One Identity Manager Web Portal 6**
 - Logging On and Off 7
 - Updating your Contact Information 8
 - Navigating around the Web Portal 9
 - Exploring Your Home Page 10
 - Using the Main Navigation 10
 - Main Content Page 11
 - Easy Navigation with Keyboard Shortcuts and Help Keys 13
 - Tips for using Web Portal 14
 - Switching Between the Mobile and Desktop Views 20
 - Hyperviews and Mobile Devices 22
- Working with the Web Portal 25**
 - Making and Managing Requests 25
 - Making a Request 26
 - Requesting through the Search Function 28
 - Requesting through a Service Category 28
 - Requesting from a Template 29
 - Requesting through a Reference User 30
 - Making Requests for Other Recipient 31
 - Renewing Requests 33
 - Resubmitting a Request 33
 - Creating and Editing Request Templates 34
 - Special Requests 35
 - Other Request Options - Request Resource 36
 - Other Request Options - Request Group 36
 - Using your Shopping Cart to Submit your Requests 37
 - Tracking your Request 41
 - Canceling Requests 42
 - Processing Pending Requests 43
 - Granting or Denying Request Approval 43
 - Handling Requests when You Need More Information 47
 - Editing Pending Requests with the Chief Approval Team 50
 - Answering Approval Inquiries 50
 - Viewing Approval History 51
 - Requesting Email Notifications 52

Delegating Roles	53
Viewing your Delegation History	55
Adding New Calls	55
Viewing Call History	55
Managing "My Responsibilities"	56
Working with Organizations	56
Working with Business and System Roles	56
Working with System Entitlements	58
Working with File System and SharePoint® Resources	62
Managing other Services	65
Claiming Ownership of a Group	66
Adding and Deleting Entitlements to Organizations, Business Roles and System Roles	67
Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services	68
Editing Master Data of Business Roles, System Roles and other Services	69
Adding Tags for Service Items	70
Adding and Editing Employees	70
Accessing Other Applications	74
Getting Information Using Views, Reports and Statistics	75
Searching in the Web Portal	75
Using the Help	76
Information about the Current Connection	76
Discovering your Statistics on the Start Page	77
What Statistics are Available?	80
Using Views to Get Information	83
Information about You and Your History	83
Your Overview	83
Contact Data	84
My Action History	84
Using the White Pages to Look Up Employees	85
My Responsibilities	85
Auditing	86
Description of Commonly Used Tabs in Views	86
Generating Reports	89
Report Subscriptions	89
Viewing Reports in the Web Portal	91
Auditing Activity and Managing Compliance	92
Auditing - Employee Details	92
Auditing - Roles and Entitlements	96

Auditing - Requests	98
Auditing - Approvals	99
Auditing - Attestations	100
Auditing - Rule and Policy Violations	101
Working with Compliance	102
Assigning Resource Owners	103
Modifying Risk Calculators	105
Performing Attestations	106
Working with Attestation Policies	106
Select Object Link Types	111
Approving and Denying Attestations	112
Editing Attestation with the Chief Approval Team	115
Viewing Completed Attestations	115
Viewing your own Attestation Policies	115
Viewing Compliance Frameworks	116
Managing Rule and Policy Violations	116
Editing Pending Violations	116
Displaying Rule and Policy Violations	118
Identifying High Risk SAP Users (Rule Analysis and Critical Function Analysis)	120
About Dell Software	121
Contacting Dell Software	121
Technical support resources	121
Index	122

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:

- Internet Information Services version 9.0 or later
- Firefox® (Release Channel)
- 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 share 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 4.0.2.5 or later
- Internet Information Services version 7 and
- Microsoft® .NET Framework version 4.5.2


 **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

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

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. Type the Web Portal URL in the address bar to Open the Web Designer 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. 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 personal 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 your name in the title bar 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

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

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:** You cannot make changes to grayed out text boxes.

To update your contact information

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**.

The tab **Contact Data** is preselected.

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

4. Click **Assign** next to **Country**.

This opens the dialog box **Country**.

5. Select the the country you want from the list.

- OR -

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

7. Click **Change** next to **Picture**.

This opens the dialog box **Picture**.

8. Click **Browse...** to find a picture.

9. Confirm your selection with **Apply**.


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

10. 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 you have selected the required area.

11. Click **Crop to selection**.

The image is cropped.


12. Click **Apply** to save the cropped area.

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


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

To edit your Active Directory® accounts


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 **Active Directory® accounts**.
4. Enable the Active Directory® user account you want if there are more than one.
5. Edit the text boxes or add new ones.
6. Click **Save** to save your changes.

 **NOTE:** This function is available if the Active Roles Module module is installed.

Navigating around the Web Portal

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

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. There are:

- 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 the arrow in the header next to the navigation path on the left.
A drop-down menu is displayed with 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:


- Main navigation menu
The function of each button in the menu bar is described to you in more detail in [Using the Main Navigation](#) on page 10.
- Page header
The page header runs across the top of the page. You can call up a view from here with your personal data, memberships, responsibilities and entitlements. For more information, see [Logging On and Off](#) on page 7, [Searching in the Web Portal](#) on page 75 and [Using the White Pages to Look Up Employees](#) on page 85.
- Breadcrumb Navigation
The 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.
- Content page
The content frame of the home page is divided into two areas. These are described in more detail in the [Main Content Page](#) on page 11.

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. After expanding the menu, you can run your task by clicking on the menu item in the menu bar or directly over the actions displayed in the main content page.

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

The following table shows the high level menus that are available to each role. Prerequisite for this is that the IT Shop configuration parameter is set in the Designer.

 **NOTE:** Which menu items you see, depends on the main menu you selected. For more information, see [Navigating around the Web Portal](#) on page 9.

The following table shows 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 1: Visible menus - header

Menu	Employees	Manager /Supervisor	External Auditor
My Profile	Yes	Yes	

Table 2: Visible menus - main menu "My Identity"

Menu	Employees	Manager /Supervisor	External Auditor
My Actions	Yes	Yes	
My Business Ownerships		Yes	
My Action History	Yes	Yes	
Service catalog	Yes	Yes	

Table 3: Visible menus - main menu "Access Governance"

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

Table 4: Visible menus - main menu "Governance Administration"

Menu	Employees	Manager /Supervisor	External Auditor
Administrator			
Governed Data			

To make approval decisions about pending items

A number is displayed beside the **My Actions**. It is the sum of all pending items for which you are responsible and require an approval decision from you. These items are displayed as submenus in **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.

1. Click in the menu **My Actions** on the menu item with a number after it.
This opens a view with list of pending items for which you must make an approval decision.
2. In the **Approval decision** column, you either check **Grant** or **Deny** in the list of pending items and then select either **Next** or **Save approval**.
This opens dialog box showing your approval decision.
3. Accept the prompt in the dialog box.
The number next to the menu item with the pending item is either decreased or no longer displayed.

Main Content Page

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 go to the

request page. On the request page, you will see the products belonging to the selected service category.

- Responsibilities

This section shows you different responsibilities statistics. 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 are shown the last 5 transacted pending requests. You can click on these requests. 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 are shown the last 5 transacted pending attestations. You can click on these attestations. 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 system

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

- Governed Data

Governing unstructured data allows for better management, including controlling the access to data, increased self-sufficiency for managers, and better data integrity.


Easy Navigation with Keyboard Shortcuts and Help Keys

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

A keyboard shortcut (also known as a key combination, shortcut, key binding, hotkey) is when several keys are pressed simultaneously or one after another on a computer keyboard. You can use keyboard shortcuts to send commands to a program, such as **Start program**, **Open file** and **Close window**. The Web Portal also provides you with keyboard shortcuts.

Simple Commands

TAB + SHIFT	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.

Helpful Shortcuts

ALT + L Sets the focus to page content

Go to start page

TAB	Navigate forwards
SHIFT + TAB	Navigate backwards
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 Software 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

Button	Navigate to the desired button with TAB key 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 Components


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 Web Portal

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

You can search, sort and filter information in the Web Portal before you display it in a view. If your view is a hyperview, 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.

Table 5: Icon Overview General

Icon	function
Search / advanced search	<p>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.</p> <p>To run a search</p> <ol style="list-style-type: none"> 1. Select either the simple or advanced search. <p> NOTE: You do not have to take case into account.</p> <ol style="list-style-type: none"> 2. Simple search: Enter the search string or part of the search string in the text box. - OR - Advanced search: Enter a search string or part of one in at least one of the text boxes. - OR - Do not enter anything. If you choose this type of search, every search result is displayed and the search process can take a long time. 3. Click Search or press Enter to run the search.
Sorting by mouse click.	<p>At the right-hand edge of a column's header there is an arrow, which you can click on to sort column contents in ascending or descending alphabetic order.</p>
Refresh	<p>To see changes in the Web Portal, you do not necessarily have to log out and log in again. You can make your changes visible by select Refresh from the current user's context menu in the header of the web application. Changes might be, for example, approvals for request or access right assignments to specific modules in Web Designer.</p>

Icon	function
------	----------

Bookmarks You sometimes have the option to set bookmarks in views in the Web Portal. Bookmarks you have set, are displayed on the start page and in the Web Portal header. Bookmarks can be deleted 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 in a list, for example, in the **System Entitlements** view under **My Responsibilities** and click **Bookmark this page**.

The bookmark is displayed on the start page and in the header.

To use a bookmark


- Click the book mark on the start page.

- OR -

Click the arrow in the header next to the bookmark icon and select the bookmark you want from the menu.

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.

- Click the link **Remove bookmark**.


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

Filtering When you click on the button, a dialog box opens where you can select different filter types.

To filter by filter criteria

1. Select the column you want to filter.


A dialog box is opened corresponding to the type of column you select.

 **NOTE:** The filter dialog boxes are differentiated by the selection of filter criteria. You can filter by text, numeric values, fixed values, such as gender, "yes" or "no", dates or objects.

2. Enter one or more search terms in **Filtering on....**
3. Select one of the following criteria from the context menu next to the text box:
 - a. **All words:**This only shows results matching all the given words.
 - b. **Begins with....:**This only shows results that being with the given character or character string.
 - c. **Ends with....:**This only shows results that end with the given character or character string.
 - d. **One or more words:**Filters by at least one of the given words.

- OR -

- Enter a value in the numeric field.

 **NOTE:** You can adjust the value using the arrows next to the numeric field.

- Select one of the following criteria from the context menu next to the numeric field:
 - a. **At least:** This only shows results which reach the given value.
 - b. **Lower than:** Only results with a lower value than the given value are shown.
 - c. **Between:** Only results between the given values are shown.

- Select the **Object filter** tab.

The dialog box is divided into **Available** and **Current**. You are offered a list under **Available**.

- Select the item you want under **Available**.


The selected item is highlighted in color and then also displayed under **Current**.

- OR -

- Click the calendar icon and select the date from the calendar or write the date in the text box.
- Select on of the following criteria from the context menu next to the text field.
 - a. **After:**This only displays the results from after this date onward.
 - b. **Before:** Only displays the results from before this date.
 - c. **Between:** Only displays items between these dates. Another text field with

1. Go to header of the filtered column.
2. Click X.

To group within a column

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


1. Select the column you want to filter.
2. Click the button **Group by column**. The column
For example, all employees with the same first name are displayed in the column **First name**, that is, Alan (3).
3. Click the arrow next to group and you see a list of all objects in the group.
4. Click the arrow next to the expanded group again to hide the list of objects.

To ungroup


- Click X next to the setting **View grouped by:**.
Reset grouped by view.

To include other columns in the table

1. Click **Additional columns** above the table.
This opens the selection dialog **Additional columns** displaying a list of additional columns.
2. Click the check box of the desired column.
This selects the column. Multi-select is possible.
3. Click **Close**.
Now you can see the column in the table and use it.

 **NOTE:** You will see the configured filter above the listed data to which you want to apply the filter.


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. Configure the settings you want for the desired column in **Filter on**.
Once you have set a filter, the filter with this setting is shown as a gray bar over the result list.
2. Click **View Settings** and select the item **Save current view** to save these settings and apply them in all tables that occur in this column.
This opens the dialog box **Save current view**.
3. Enter in a name for the filter setting and click **Save**.

You can select the filter you added in the **View Settings** menu.

To delete a saved view


 **NOTE:** You can tell if the saved view is active by the gray bar with the filter setting described in it which appears above the result list. The filter you can also see the filter you set in **Filter on**.

1. Click **View Settings** and select **Edit list** from the menu.
This opens the dialog box **Edit view settings**.
2. Click **Delete** next to the name of the view setting you want to delete.
The delete view setting is removed from the dialog box and you cannot select in the menu anymore.

Eraser The eraser delete the text entered in the text box.

Export this 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 91.

To export a view

 **NOTE:** Before you export a view, you can add more columns to it, if required, using **Additional columns**.

1. Click **Export this view** in the view.
This opens the dialog box **Export this view**.
2. Enable the following setting:
 - a. All pages
 - b. Remove header row
3. Select either the option **Export as PDF**.
- OR -
4. Select the option **Export as CSV**.
5. Click the **Export** button.
The corresponding report is generated and displayed according to your settings or you are asked whether you want to save o open the report.

Icon	function
Hyperview	<p>A hyperview is a graphical representation of relations between different elements from One Identity Manager. You can see an example of a hyperview on your Overview tab, which you will find above your user name in the title bar of the web application. The shape Employee is the main shape in the hyperview and contains information such as contact data and memberships. All other information about yourself as an employee is represented in other shapes surrounding the main shape.</p> <p>To change how a hyperview looks</p> <ol style="list-style-type: none"> 1. Click one of the shapes and move it on your screen. 2. Click the button at the top right of the shape if the expand button is available. <p>You can view other detailed information in the expanded view.</p> <p>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.</p> <p>The operating option for hyperviews are more complex in the web application's mobile view and are described in a separate chapter. For more information,, see Hyperviews and Mobile Devices on page 22.</p>
Actions	<p>You will see the Actions link on a number of pages and main views. This link contains a context menu which provides you with various actions. The types of action are always different depending on the current view you are currently working with. Use the Actions link to select an action which applies to all items within this view. Selecting an action in the main view only effects the currently selected item.</p>

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 about optimizing your display, see [Getting Started with the One Identity Manager Web Portal](#) on page 6.

To change to the mobile view

1. Click the arrow next to the info icon in the Web Portal 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 6: Icon for Navigating in the Mobile View

Icon	Function
	<p>Use this button to hide or show the navigation menu. If your mobile device has a touchscreen, you can swipe over or tapping the display to use the navigation menu.</p> <p>To open the navigation menu</p> <ol style="list-style-type: none">1. Tap this button on the screen. - OR - Touch the screen with a finger and drag from left to right. This opens the navigation menu. <p>To close the navigation menu</p> <ol style="list-style-type: none">1. Tap the button on the screen again. - OR - Touch the screen with a finger and drag from right to left. This closes the navigation menu.
	<p>Use the Back button to return to the previous view in your web application. It has the same function as the Back button in your browser.</p>
	<p>Use this button to update the view. Actions running in background supply new values if required.</p>
	<p>Tap either the icon or user names to display your user's Overview. Use the tabs Permissions, Resource access and Attestations to view more information.</p>
	<p>Use this button to log out of the web application.</p>
	<p>Tap this button to expand the menu with bookmarks.</p>

Icon	Function
	<p>Through this menu, you can reach the Properties menu with more menu items. This menu is identical to the menu Info in the desktop view title bar with the exception of the menu item My Settings. The menu items are as follows:</p> <ul style="list-style-type: none"> • My Settings • Telephone book • Help • Connection • Switch to desktop view • Info

This menu can also be used by swiping or tapping the screen

To open the "Properties" menu

1. Tap **Properties** on the screen.
- OR -
- Touch the screen with a finger and drag from right to left.
This displays the menu **Properties**.

To close the "Properties" menu

1. Tap **Properties** on the screen again.
- OR -
- Touch the screen with a finger and drag from left to right.
The **Properties** menu is closed.

To switch to the desktop view

1. Tap **Properties** in the Web Portal's title bar (see table).
This opens a menu with other menu items.
2. Select **Switch to desktop view** by tapping on it.
The view switches to the desktop view.

Hyperviews and Mobile Devices

In the mobile version of your web application there are more operating options available as in the desktop version you are used to. In the section below, we shall name and describe the operating options for hyperviews. Other general operating options in the mobile version are described in a separate chapter. For more information,, see [Switching Between the Mobile and Desktop Views](#) on page 20.

To move a shape

1. Touch the shape on the screen with your finger and drag it to the new position.

To move a hyperview

1. Touch the screen with your finger and drag the hyperview to the new position.

To zoom in or out on a hyperview



TIP: If your mobile device does not have a touch screen, move the hyperview 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.

1. Touch the screen with two fingers anywhere and move your fingers apart.
The entire hyperview is zoomed in.
- OR -
2. Touch the screen with two fingers anywhere and move your fingers together.
The entire hyperview is zoomed out.



NOTE: You can only zoom in or out by a fixed factor.

To zoom in or out on a hyperview by double tapping

1. Double tap anywhere on the screen.
The hyperview zooms in by a fixed amount.
2. Double tap again anywhere on the screen.
The hyperview zoom out by a fixed amount.

To expand or collapse a shape



NOTE: The main shape or central shape in the hyperview is always expanded and cannot be collapsed. All other shapes are collapsed when the hyperview is loaded.

Shapes that have a button at the top right can be expanded. You can view other 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 the shape.
The shape is expanded and you can see the entire contents.
2. Tap on the shape's header.
This collapses the shape.

To zoom in or out on a shape

1. Touch the shape on the screen and hold your finger on this point.
The shape zooms in by a fixed amount.
2. Remove your finger from the screen.
The shape returns to its original size.

To make all the hyperview's shapes visible on the screen

- Tap **Overview** on the screen.

The hyperview changes its size so that as many of the shapes are visible on the screen.

To return the hyperview to its original size

- Tap **Center** on the screen.

The hyperview is displayed in its original size again.

To expand or collapse all hyperview shapes at once

1. Tap **Expand**.

All shapes in the hyperview are expanded at the same time. Now you will see the button **Collapse** instead of **Expand**.


2. Tap **Collapse**.

All the hyperview shapes are collapsed at the same time.


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 portal is customized to suit you. Its functionality is dependent on your roles and ownerships.

- [Making and Managing Requests](#)
- [Delegating Roles](#)
- [Managing "My Responsibilities"](#)
- [Adding and Editing Employees](#)
- [Accessing Other Applications](#)

 **NOTE:** For information specific to auditing or compliance, see [Auditing Activity and Managing Compliance](#) on page 92.

Making and Managing Requests

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

You can request a variety of products in the Manager, depending on your company's implementation. For example, you may be able to request:

- Group or system entitlements (for example, Active Directory®, SharePoint®, Lotus Notes®, SAP 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**.

For more information, see:

- [Making a Request](#)
- [Using your Shopping Cart to Submit your Requests](#)
- [Tracking your Request](#)
- [Processing Pending Requests](#)

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 a Service Category](#)
- [Requesting from a Template](#)
- [Requesting through a Reference User](#)
- [Making Requests for Other Recipient](#)
- [Resubmitting a Request](#)
- [Special Requests](#)



NOTE: Requestable products have been configured and made available by an administrator in the IT Shop. Products are configured by assigning request properties and determining associated products and/or optional products. For more information, see the IT Shop.

To renew a request

1. Click **Service Catalog | Renew**.
All request are shown without taking time limits into account. You can sort the requests by validity to find those that need renewing, more quickly.
2. If you are renewing a request in the name of another employee, see [Making Requests for Other Recipient](#) on page 31.
3. Enable the check box next to the request you want to renew and click **Renew**.
This opens the dialog box **Renew**.
4. Enable the check box next to **Valid until** and click on the calendar icon.
This displays a calendar.
5. Select the renewal date.
6. Enter a reason for renewing in the reason box.
7. Click **Save**.
The request is moved to your cart. For more information, see [Using your Shopping Cart to Submit your Requests](#) on page 37.

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

1. Click **Service Catalog | Request**.
2. Click the service category **Groups.Active Directory®**
3. Enable the check box against the desired product in the list.

Further information about the product is shown to the left of the main content.

4. Click **Request** if you want to add more products to the cart.

- OR -

Click **Submit request now**.

This opens a dialog box with a text box.

5. Enter your information about the group in **Group name** 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.

To request a product with dependent products

Example: paper and cartridge for a printer are requested together. There is a condition here that the color cartridge may only be requested once a month. You can always request paper. Your paper is nearly out and you must repeat the request before month end when you would have to start the request over again. You can request paper without having to request a color cartridge.

1. Select **Service Catalog | Request** and the corresponding service category for your request.

This displays the **Request** view with a list of available products.

2. Select the product from the list and click **Request**.

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



NOTE: If the dependent product has not been requested as yet, it is automatically requested as well. Use the arrow next to the requested item to display the additional products again.

3. Click the arrow next to the request of the dependent request pr

Another item appears below the request.

- OR -

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



NOTE: You can only enter one reason in the main content view for this item and set **Valid from** and **Valid to** and then save.

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

To add more information to a request

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

The view **Cart Templates** is displayed.



TIP: If you click on the arrow next to the template, the contents of the template are displayed and single items can be deleted if required.

2. Select your template and click in **Additional information** in the **Actions** column.

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

3. Enter the additional information you want and check the required options.

4. Click **Save**.


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 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 about added keywords, see [Adding Tags for Service Items](#) on page 70 or the IT Shop Guide.

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

1. Click **Service Catalog | Request**.
2. Enter the keyword or part of it in **Product** in the **Request** view and click **Search** or **Search in all categories**.

This displays a list of service items found. For more information about completing the request, see [Requesting through a Service Category](#) on page 28.

 **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 the keyword or part of it in **Product** in the **Request** view and click **Search**.





An overview is displayed with the resulting service item within the selected service category. For more information about completing the request, see [Requesting through a Service Category](#) on page 28.

Requesting through a Service Category

You can make requests through service categories on the content pages of the menu **Service Catalog** or the submenu **Request**. After you have selected a service category, you may be presented with other subgroups and a list of all products in this service category. If you select a subgroup, you are presented with a list of all the products in this subgroup. The listed products can be filtered by search term or group. For more information, see [Using your Shopping Cart to Submit your Requests](#) on page 37.

There maybe products in the list of all products that are displayed with an icon. The meanings of these icons are explained with relevance to the product, in the table below:

Table 7: 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 has already been assigned to the user, for example, through inheritance. 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. Click **Service Catalog | Request**.

The **Request** is shown with other options.



NOTE: As long as you have not made a select for a request, the message **Browse the categories or search the catalog to find what are you looking for** is displayed.

2. Click on the service category, on the main content page, from which you want to make a request.

The selected service category is displayed as a link in the main content **Request** view and the products contained are listed. If the selected service category has other groupings, an arrow button appears next to the link, which you can click on to show more options.

3. Click the arrow again to limit the options displayed.

4. Select the item you want from the context menu.

- OR -

5. Enter the name of the product you are searching for in **Product** and click **Search** or **Search in all categories**.

This displays the product.

6. Click **Request** in selected product's row.

- OR -

7. Enable the check box in the **Request** column for all products you want to request.

8. Click **Submit request now**.

This opens a dialog box for the requested product.

9. Enter more information about the product in the text box and confirm with **OK**.

Your request is listed in the **My Shopping Cart** view. You can enter more information or run other actions on the main content view. The products are added to the shopping cart. You remain in this view and can add more products to your request.

- OR -

10. Click **Submit request now**.

Then your shopping cart is shown. For more information about the menu item **Shopping Cart**, refer to [Using your Shopping Cart to Submit your Requests](#) on page 37.

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. You do not have to request all products included in the template: You select the products you want from the template. For more information on templates, see [Creating and Editing Request Templates](#) on page 34.

To make a request using a template

1. Click **Service Catalog | Request**.
2. Click **Actions** in the bottom section of the page and select **Select a request template** from the submenu.
This opens the dialog box **Select template**.
3. Click the arrow to the left of the request template name to get more information about this template.
You can see more information about the products in the template by expanding it further.
4. Click the request template's name to display details of the template.
This opens the dialog box **Template details**.
5. Select the template you want and click **Select**.
This template is checked on the page **My Shopping Cart** with more details displayed in the main content view.
6. Enter a reason in the reason box and enter dates in the calendar is necessary.
7. Execute the following actions:

- 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 item contained in the shopping cart.

- OR -

- b. Click **Check and submit shopping cart**.

The request is checked and the dialog box **Submit shopping cart** is show. Confirm the prompt with **OK**.

For more information about the menu item **Shopping Cart**, refer to [Using your Shopping Cart to Submit your Requests](#) on page 37.

Requesting through a Reference User

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

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

1. Click **Service Catalog | Request**.
2. Click the link next to **By reference** in the main content.

This opens the dialog box **Employee**. A selection of authorized users is displayed.



NOTE: To display staff details, click on **Additional columns**. This opens the dialog box **Additional columns** with a selection of other options.

3. Select an employee from the list or select an entry from **Recently selected**.

This lists requests, memberships and entitlements depending on what this employee has previously requested or in which organization memberships o similar exist.


4. Enable the check box next to the item you want in the list (multi-select is possible) and click **Add to shopping cart** or press **Enter** or **Return** respectively.

Then your shopping cart is shown. For more information about the menu item **Shopping Cart**, refer to [Using your Shopping Cart to Submit your Requests](#) on page 37.

Making Requests for Other Recipient

If you have the necessary permissions, for example, as department manager, you can make requests for other employees. You can make the same request for multiple other employees at the same time. You will find out how to request for multiple recipients here.

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


 **NOTE:** You can sort and filter some views to help you locate products or requests. For more information, see [Tips for using Web Portal](#).

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. Click **Service Catalog | Request**.
2. Click the link next to **Recipient** in the main content.

The **Recipient** view is shown with a list of employees in alphabetical order. This view is divided into two sections. In the **Online** section is a list of users for you to select from. Select users are listed in the section **Up to date**.

 **NOTE:** To display staff details, click on **Additional columns**. This opens the dialog box **Additional columns** with a selection of other options.

3. Select the employee you want from the list by clicking on it (multi-select is possible).

The selected users are moved to **Up to date**. In **Available** section, the icon next to the user changes.

4. Click **Close**.

The **Recipient** view is closed and the selected employees are shown under the already selected recipients.

5. Request products using one of the options already described:
 - [Requesting through a Service Category](#)
 - [Requesting from a Template](#)

To copy a request

1. Click **Service Catalog | Shopping Cart**.
2. Mark the request you want on the **My Shopping Cart** page.
3. Select **Request for multiple employees** under **Actions** in the main content view.

The **Request for multiple employees** dialog box opens with a list of employees in alphabetical order. This view is divided into two sections. In the **Online** section is a list of users for you to select from. Select users are listed in the section **Up to date**.

4. Select the employee you want from the list by clicking on it (multi-select is possible).
The selected users are moved to **Up to date**. In **Available** section, the icon next to the user changes.
5. Click **Save**.
The **Request for multiple employees** is closed and the requests for the selected employees are displayed under the requests already listed.

To add products to a request

1. Click **My Actions | Pending requests**.
2. Mark the request you want on the **Pending Requests** page.
3. Select **Show entire request** under **more** in the main content view.
You will see the selected request on the page **Request overview**.
4. Click **Add items to this request** in the main content view.
The **Request** page is displayed with the available products.
5. Select the product you want.
The selected product is added to the cart.
6. Click **Check & submit shopping cart** to complete the request.
You can also add more items to your cart. For more information, see [Using your Shopping Cart to Submit your Requests](#) on page 37.

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 user can only be confirmed if a special approval workflow is explicitly set up for the requested product.

1. Click **My Actions | Pending requests**.
The request you can approve are shown in the view **Pending Requests**.
2. Mark the request, which requires confirmation of the terms of use by the requester,
In the main content view, you can see, amongst other things, information about approval decisions for requests and terms of use on the **Workflow** tab.
3. Enable **Approve** or **Deny** in the **Decision** column.
4. Click **Next**.
The view **Approvals** view appears displaying the corresponding approval decision.
5. Enter in **Reason for denials** or **Reason for approvals** a reason for your decision.
- OR -
6. Select a reason in **Standard reason**.
7. Click **Save approvals**.

Renewing Requests


Some requests are only valid for a limited period. In this case, you can apply for a renewal of the 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 request expires, therefore, giving you the chance to renew. The requests are automatically canceled once they have expired.

To renew a request

1. Click **Service Catalog | Renew**.

All request are shown without taking time limits into account. You can sort the requests by validity to find those that need renewing, more quickly.

 **NOTE:** Read the chapter [Requesting through a Reference User](#) on page 30 if you want to make requests for other users.

2. Click **Show request** next to the request you want to view the entire request and other details.

The view **Request overview** is displayed.

 **NOTE:** To return to the **Renew** view, click **Service Catalog | Renew** or **Back** in the preview toolbar.

- OR -

3. Select the request you want to renew and click **Renew**.
4. Select an expiry date.
5. Enter a reason the request in the reason box.
6. Click **Save**.

The request is moved to your cart. For more information, see [Using your Shopping Cart to Submit your Requests](#) on page 37.

Resubmitting a Request

If a request was canceled, aborted or denied, you can resubmit the original request, which can be faster than generating a new request, and preserves the history of the request.

To resubmit a request

1. Select **My Action History | Request History**.

This displays the view **Request History**.

2. Select the desired request from the **Request History** view.

More information is displayed about the request in the main content view.

3. Click **Submit again**.

4. Enter a reason for submitting the request again in the text box and click **OK**.

The request is added to your cart. For more information, see [Using your Shopping Cart to Submit your Requests](#) on page 37.

To search in the request history


1. Click **Advanced search** in the **Request History** view.

This displays more search settings in the **Request History** view.

2. Set the following search options:
 - a. **Display requests:**Enable one or more check boxes with different options to limit the search.
 - b. **Filter by product name:**Enter a product name in the text box.
 - c. **Filter by request number:** Enter the request number in the text box.
 - d. **Request state:**Enable one or more check boxes with different options to limit the search.
3. Click **Search**.




The search is carried out and all requests found taking the search settings into account are displayed in **Request History**.

Creating and Editing Request Templates

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

This menu item shows you all templates you have created yourself and system-wide templates (created and published by others). Use the arrow next to the request template to expand it and reveal the list of products it contains. For information on using templates, see [Requesting from a Template](#) on page 29.

Table 8: Templates - Status

Status	Meaning
	This template has not been approved yet. A decision about publishing it still pending.
	This template has been marked for publishing but has not yet been granted publishing approval from an authorized approver.
	This template has been approved for publishing by an approver.

To create or edit a request template

1. Place your request in your cart or the cart of another recipient.

For more information, see [Tracking your Request](#) on page 41.

2. Open the view **My Cart**.



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

3. Click the action **Create template from shopping cart** in the **My Shopping Cart** view.

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.

4. Select a request template from the list of exiting request templates and click on **Select**.

- OR -

Enter a name for the new request template in **Name of the new template** under the list of request templates.

5. Click **Create template**.

To delete an item or an entire template

1. Select **Service Catalog | Maintain Templates**.
2. Select your template and click **Delete** in **Actions** column if you want to delete the entire template.
- OR -
3. Click the arrow next to the request template.
The template is displayed with all the items it contains.
4. Mark the item you want to delete from the template and click **Delete** in the **Actions** column.
5. Click **Yes** in the confirmation dialog box.

To delete a product from a template

1. Select **Service Catalog | Maintain Templates**.
2. Click the arrow next to the desired template to display all the items.
3. Click **Delete** in the **Actions** column of you want to delete the item.
You can only delete your own templates.
4. Click **Yes** in the confirmation dialog box.

To share your template with other users

1. Select **Service Catalog | Maintain Templates**.
2. Select your template and click in **Additional information** in the **Actions** column.
3. Enable the check box **Template is available to other employees**.
4. Enable the **Template has been approved** check box.



NOTE: Do not Enable this box, if you would like to make further modifications to your template before making it available for use. Make any modifications, and then check **Template has been approved** to approve the template.

5. Click **Save**.

To add more information to a request

1. Select **Service Catalog | Maintain Templates**.
2. Select your template and click in **Additional information** in the **Actions** column.
3. Enter the additional information in **Description**.

Special Requests

Running certain actions in Web Portal triggers request that are added to the shopping cart. The following actions cannot be run from the **Request** menu:

- [Adding and Deleting Entitlements to Organizations, Business Roles and System Roles](#) on page 67
- [Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services](#) on page 68
- [Editing Master Data of Business Roles, System Roles and other Services](#) on page 69

Other Request Options - Request Resource

If you use a service category to make a request, the service category **Resource Access** plays a special role. Both the products **File system access** and **SharePoint® access** are available. Both products are requested using the same method. The requester requests access to the resource required.

To make a request in the service category "Resource Access"

1. Click **Service Catalog | Request**.
2. Click on the service category **Resource Access** in the main view.
The selected service category is displayed as a link in the main content **Request** view and the products contained are listed. If the selected service category has other groupings, an arrow button appears next to the link, which you can click on to show more options.
3. Click the arrow again to limit the options displayed.
4. Select the item you want from the context menu.
- OR -
5. Enter the name of the product you are searching for in **Product** and click **Search** or **Search in all categories**.
This displays the product.
6. Enable the check box against the desired product in the list of resources displayed.
7. Click **Request** in the **Request** column.
- OR -
8. Click **Submit request now**.
This opens a dialog box with other settings and editing options. This dialog box is divided into two sections. In the **Available** section is a list of resources for you to select from. Selected resources are displayed in the **Current** section.
3. Enable the check box **Enter path manually** if you have selected a resource from the category **File system access** and enter the path manually in the text box.
4. Click the link next to **Managed host** in the dialog box.
This opens the **Managed host** dialog box.
5. Select a **host** and click **Close**.

Other Request Options - Request Group

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

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

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

1. Click **Service Catalog | Request**.
2. Click on the service category **Groups** in the main view.**Active Directory®**
3. Enable the check box against the desired product in the list of groups displayed.
4. Click **Request** if you want to add more products to the cart.

- OR -


Click **Submit request now**.

This opens a dialog box.


5. Enter your information about the group in **Group name** 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

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

Your requests are stored in your shopping cart until you are ready to submit them. Each request in your shopping cart is listed, including previously saved requests. All requests made in a session are grouped together and assigned a shopping cart identification number. You can save requests for later to and execute them another time.



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


Use the **Check only** button to find out whether the requester has the permissions required to request this product or whether a compliance rule will be violated by the request. After the test, a dialog box opens asking whether the request should be carried out.

 **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. If such a case occurs, you can see the compliance violation in the **Status** column of your shopping cart and in the main content view.

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




Table 9: Status of your Check

Icon	Status
	Request can be made.
	Request violates a rule but can still be made.

Icon	Status
	Request cannot be made due to missing request permissions.

Advice If the request verification is still pending, a advice notice is shown in the main context view.

The **Request** menu contains several buttons and options which you can use to edit your requests. The buttons and actions are explained in the following tables:

Icon/Button	Action
Text boxes	<p>These text boxes are an aid for adding additional information, such as, request properties. This additional data could be, for example, that a request violates a compliance rule under specific conditions. You will see the text boxes in the dialog box after you have selected the product in the Request menu and made the request. Other places where you can find these text boxes are:</p> <ul style="list-style-type: none"> • In your shopping cart • On your saved for later list • On your request template
	<p>This button delete the request from your:</p> <ul style="list-style-type: none"> • Shopping cart • Saved for later list • Request template
	<p>This button saves your additionally edited information in the main content view of your request.</p>
Request for multiple employees	<p>With this action you can duplicate requests in your shopping cart for other employees. You will find this action in the context menu Actions in the main detail window. For more information, see Making Requests for Other Recipient on page 31.</p>
Save for Later	<p>With this action you move the request from your shopping cart to a "saved for later" list. If the saved for later list was empty until now, a new tab Saved for later appears next to the shopping cart. You will find this action in the context menu Actions in the main detail window.</p>
	<p>This icon is on the request's start page. For example, in the list of requests or in the main content view of a request you have previously marked. It provides you with up-to-date information about the request.</p>
Check only	<p>With this action requests in your shopped cart are tested. After you clicked Check only in context menu Actions in the My Shopping Cart view, the listed requests are labeled with the status OK and the information that the request can be made appears in the main content view.</p>
Create template from shopping cart	<p>You have the option to save the current state of shopping cart as a template for other requests, for example, for other recipients.</p>
Delete invalid requests	<p>With this action you can delete requests from your shopping cart that either violate a rule or have insufficient permissions. You will find this function in the context menu in My Shopping Cart.</p>
Delete shopping cart	<p>With this action you can delete the entire contents of your shopping cart with one click. You will find this function in the context menu in My Shopping Cart.</p>

Icon/Button	Action
Edit shopping cart	Use this button you can edit your shopping cart. You can, for example, save requests for a submission later.
Check and submit shopping cart	Use this button you can check and submit your shopping cart with one click. You will find this function in the context menu in My Shopping Cart .

If your cart does not contain any products, you can select one of the following options:

- Find products for your shopping cart
If you click on this link, you are navigated to the menu item **Request**. For more information,, see [Making a Request](#) on page 26.
- View the request history
If you click on this link, you are navigated to the **Request History** view under the **My Action History** menu. For more information,, see [Using Views to Get Information](#) on page 83.


To view your shopping cart

1. Click **Service Catalog | Shopping Cart**.
- OR -
Click in the menu bar **Shopping Cart**.
You can only see these options if there are requests in your shopping cart.
2. Use the options in the **My Shopping Cart** view to choose how to display the contents of your cart.

To save a request for later processing

1. Select the desired request from your shopping cart.
2. Click **Actions** in the main content view.
This shows a menu with menu items.
3. Select **Save for later**.

To place a request in the shopping cart

 **NOTE:** The tab for items saved for later is only shown in **My Shopping Cart** if at least one request has already been saved for later.

1. Select the request in list of items saved for later.
2. Click **Actions** in the main content view.
This shows a menu with menu items.
3. Select **Add to cart**.
This moves the request into your shopping cart.
4. Select **Service Catalog | Shopping Cart** in the menu bar.
5. Select the transfer requests in **My Shopping Cart** and click on one of the available actions in the main content view, for example **Add to cart**.
- OR -
6. Select the **Action** tab in **My Shopping Cart** to select more products for the cart.

To request for multiple employees

1. Open **My Shopping Cart**.
2. Select the requests you want.
3. Select **Request for multiple employees** under **Actions** in the main content view.
This opens the dialog box **Request for multiple employees**.
4. Select from the list of other employees and click **Save**.





To delete a request from your shopping cart

1. Select the request to delete in your shopping cart and click **Delete this request** in the main content view.
- OR -
Select the group to delete, if the shopping cart view has been group and click the link **Actions** in the **My Shopping Cart** view and select **Delete shopping cart** in the menu.
2. Click **Yes** in the dialog box.

To delete all current requests from your cart

1. Select **Delete shopping cart** under the **Actions** in the **My Shopping Cart** view.
This opens a dialog box with the request.
2. Click **Yes** in the dialog box.


To submit your requests

1. Open **My 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 34.
3. Select the request you want and edit the information in the main content view if required.
 **NOTE:** The request must have been checked and status set to **OK**.
4. If you would like to make a comment on the cart, or add a reason for requests, Click **Edit shopping cart**.
5. Enter the information and click **Save**.
 **NOTE:** You can choose to perform a check on you requests at any time by clicking **Check only**. Your request is submitted for processing, and may require a manager's approval.
6. Click **Check and submit shopping cart**.
This opens a dialog box for the shopping cart.
7. Confirm the prompt with **OK**.
 **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 check the box **I have read and understood the terms of use**. You may be prompted to enter your user name and password. Click **Accept** to close the terms of use view and continue with the request. For more information, 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 **My Shopping Cart**.
2. Click **Edit Shopping Cart** if you want to edit several requests at the same time.
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 there is already a date in **Valid from**, the validity period is determined as from this date and not from the approval date. If the request approval validity period has expired, an error message is displayed and the request is aborted.

4. Click **Save** to save the dates.



Tracking your Request

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

All requests that you have made or another person has made for you, are listed in your request history. You can limit the request history view, using the filters shown in column or using different search criteria.

The following statuses may be shown in the request history **Compliance** column:

Table 10: Compliance Status in the Request History

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

When you mark a request, the request's status, amongst other things, is shown in the main content view. Possible views are:

Table 11: Request Status in Main View


Status	Description
Requested	Request is being processed.
Assigned	The request has been assigned to you.
Denied	The request was denied. Reason for being denied is a policy or rule violation or if a manager has not checked the request.
Unsubscribed	Request has been canceled. For more information, see Canceling Requests on page 42.
Aborted	The system was not able to carry out the request. This case occurs no one was responsible for checking the request or if the validity period had expired. The request history is displayed with the reason for aborting.
Renewal	The request was renewed. Select the effected request in the main content view to see more information about renewals on the Information tab. There you can see who dealt with the renewal and when.

More information about the request is available in the main content view on the tabs **Information**, **Compliance** and **Workflow**.

To view the current status of your request


1. Click **My Action History | Request History**.
2. View the current status of your requests in the **Compliance** column.
3. Mark the desired request and view more information in the main content view for the request.
4. Select a tab to explicitly view the appropriate information in chronological order.

To abort a request from the request history


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

1. Do the same as in **To view the current status of your request**.
2. Click **Withdraw request** in the main content.
This opens the dialog box **Cancel request**.
3. Enter a reason for aborting in the text box.
4. Click **OK**.

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

 **NOTE:** You can resubmit unsubscribed, aborted or denied requests with the **Submit again** button. If not, the button is not visible in the main content view.


Canceling Requests

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

There are two ways to cancel a request:

- **Withdraw**
- **Unsubscribe**

Use the **Service Catalog** or **My Action History** to withdraw a request. 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 withdraw a request

1. Click **My Action History | Request History**.
2. Select the request
. Only requests with the status **Request** can be withdrawn.
3. Click **Withdraw request** in the main content.
4. Enter a reason for canceling in the text box and click **OK**.

To unsubscribe products

1. Click **Service Catalog | Unsubscribe**.
2. Enable the box next to the request you want to unsubscribe.
3. Click **Unsubscribe**


This displays the **Unsubscribe** dialog box.

 **NOTE:** Use the action **Show entire request** to display the other products linked to this request.

4. Enter a reason for unsubscribing in the text box.
5. Click **Save**.

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

Processing Pending Requests


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

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.

- [Granting or Denying Request Approval](#)
- [Handling Requests when You Need More Information](#)
- [Viewing Approval History](#)

Granting or Denying Request Approval

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. If you are ready to make your decision, you can grant or deny approval for a 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 Web Portal](#) on page 14.

 **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 standard 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. For more information, see [Viewing Approval History](#) on page 51. If you are not ready to make your approval decision, see [Handling Requests when You Need More Information](#) on page 47

To approve a single request

1. Click **Start**.

The start page is displayed. In **Pending Requests** is a list of the most recently transacted requests still pending approval. Click on one of the listed items to view the request.


 **TIP:** Use the link **Show all pending requests** to view all pending request at a glance.

2. Mark the desired request in the list.

This displays details of the request in the main content view.

3. Enable **Approved** in the **Decision** column and click **Next**.

This displays the **Approvals** view. In this view you see the request that you have marked for approval.

 **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**.

4. Enter a reason for granting approval in in **Reason for approval** or select a reason in **Standard reason** and click **Save approvals**.

The search is carried out and all requests found taking the search settings into account are displayed in **Approval History**.


To deny a request

1. Click **My Actions | Pending requests**.

2. Mark the request you want to deny in the list of pending requests.

3. Enable **Deny** in the **Decision** column and click **Next**.

This displays the **Approvals** view. In this view you see the request that you have marked for denying approval.

 **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**.

4. Enter a reason for denying approval in in **Reason for denial** or select a reason in **Standard reason** and click **Save approvals**.

The search is carried out and all requests found taking the search settings into account are displayed in **Approval History**.

To view a complete request and approve all pending requests

1. Click **My Actions | Pending requests**.

2. Mark the request you want to grant or deny approval for in the list of pending requests.

3. Click the arrow next to **more...**

4. Select **Show entire request**.

The view **Request overview** is displayed with details of the request. You can add more items to your request.

5. Click **Approve all** if you want to approve all pending requests.

All the requests are granted approval.

6. Click **Export this view**.

This opens the dialog box **Export this view**. You can set various options before you export the view.

To make approval decisions about pending requests

1. Click **My Actions | Pending requests**.
2. Mark the request you want to grant or deny approval for in the list of pending requests.
3. Enable **Approve** or **Deny** in the **Decision** column and click **Next**.

Some requests require more information before an approval decision can be made. In this case, you can view information about the pending request on the right-hand side of the main content in **Pending Requests**. The tab **Information** provides you with information about the product, recipient and requester, amongst others. Previously stored data is displayed under the product name in the list of pending requests. On the **Workflow** tab, you can see lifecycle of the request in chronological order. The **Compliance** tab shows you any rule violation for this request. For more information, see [Handling Requests when You Need More Information](#) on page 47.


4. Click **Next**.

This displays the **Approvals** view. In this view you see the request that you have marked.

5. Enter a reason for your decision in **Reason for approval** or **Reason for denial** or select a reason in **Standard reason** and click **Save approvals**.

Your reason helps provide an audit trail for requests


6. Enter the **Valid until** expiry date for the request if required.

 **NOTE:** This option is only available when approving a request.

7. Click **Save approvals**.

To make approval decisions about requests from the service category “Resource Access”

1. Click **My Actions | Pending requests**.
You will see an lists of requests pending your approval.
2. Check the request dealing with the resource access.

 **NOTE** The system automatically assigned the resource to a group. If the resource does not fit in the group, you can change the group manually with the **Select a group** button. If the manually assigned group does not fit, a compliance violation results.

3. Enable the check box **Approve** or **Deny**.

Some requests require more information before an approval decision can be made. In this case, you can view information about the pending request on the right-hand side of the main content in **Pending Requests**. The tab **Information** provides you with information about the product, recipient and requester, amongst others. Previously stored data is displayed under the product name in the list of pending requests. On the **Workflow** tab, you can see lifecycle of the request in chronological order. The **Compliance** tab shows you any rule violation for this request. For more information, see [Handling Requests when You Need More Information](#) on page 47.

i | **NOTE:** Pending requests, which have been denied approval (whether from an approver or automatically) are displayed in the view **Pending Requests** with a reason. 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 main content of the selected request.

4. Click **Next**.

This displays the **Approvals** view. In this view you see the request that you have marked.

5. Enter a reason for your decision in **Reason for approval** or **Reason for denial** or select a reason in **Standard reason** and click **Save approvals**.

Your reason helps provide an audit trail for requests

6. Enter the **Valid until expiry date** for the request if required.

i | **NOTE:** This option is only available when approving a request.

7. Click **Save approvals**.

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

1. Click **My Actions | Pending requests**.

You will see an lists of requests pending your approval.

2. Check the request dealing with the new Active Directory Module request.

3. Select the **Information** tab in the main content if it is not already pre-selected.

4. Click **Configure the new group** to enter or change the data in **Container**, **Name** and **Scope**.

This displays the dialog box **New Active Directory security group**.

5. Enter the name for the new group in **Name**, if required.

6. Click the link **Change** or **Assign** next to **Container** if required.

7. Select a group type in **Group type**, if required.

8. Click **OK**.

This closes the dialog box.

9. Enable the check box **Approve** or **Deny**.

Some requests require more information before an approval decision can be made. In this case, you can view information about the pending request on the right-hand side of the main content in **Pending Requests**. The tab **Information** provides you with information about the product, recipient and requester, amongst others. Previously stored data is displayed under the product name in the list of pending requests. On the **Workflow** tab, you can see lifecycle of the request in chronological order. The **Compliance** tab shows you any rule violation for this request. For more information, see [Handling Requests when You Need More Information](#) on page 47.

i | **NOTE:** Pending requests, which have been denied approval (whether from an approver or automatically) are displayed in the view **Pending Requests** with a reason. 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 main content of the selected request.


10. Click **Next**.

This displays the **Approvals** view. In this view you see the request that you have marked.

11. Enter a reason for your decision in **Reason for approval** or **Reason for denial** or select a reason in **Standard reason** and click **Save approvals**.

Your reason helps provide an audit trail for requests

12. Enter the **Valid until expiry date** for the request if required.


 **NOTE:** This option is only available when approving a request.

13. Click **Save approvals**.


Handling Requests when You Need More Information

If you are not able or prepared to make a decision on a request, you can:

- Edit the reason on a pending request.
- Request more information from another employee.
- Reroute the request to another approver.
Note that this is only an option if the product is configured by an administrator to allow for this.
- Relegate the approval to another employee, if delegation is enabled for you on the request.
- Add more approvers to the list, if you have the authority to do so.

 **NOTE:** You can optionally select a predefined text from **Standard reasons** using the link **Assign** for all requests still to be approved. The standard reason provides additional information to the reason given in **Enter information for the new group** in the main content, Standard reasons are displayed in the approval history and in the case details.

To edit the reason of a pending request

 **NOTE:** You must read the reason and edit it if necessary before you, as approver, can edit a pending request for adding a new group.

1. Click **My Actions | Pending requests**.
2. Mark the request you want to edit in the list of pending requests.
3. Click the link **Supply information for the new group in the main content** in the main content.
This opens a dialog box with text box and other settings.
4. Enter the required data in the text box and select one or more setting options.
5. Confirm with **OK**.

To ask a question

1. Click **My Actions | Pending requests**.
2. Mark the request you want to edit in the list of pending requests.
3. Select **Ask for help** under **more** in the main content view.
This opens the dialog box **Submit an inquiry about this request** showing a list of employees.

4. Select an employee from the list.

- OR -

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



NOTE: For more information about using the filter function, see [Tips for using Web Portal](#) on page 14.

5. Click **Select** next to the employee you are looking for in the list of employees or in the result list, respectively.

This opens the dialog box **Submit an inquiry about this request**.

6. Enter your question about the request in **Your question**.

7. Click **Save** to send the question.

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

To delete a question

1. Select the request for which you have already submitted a question.

2. Click **Recall last question** in the main content view.

This opens the dialog box **Recall last question**.

3. Enter a reason for recalling the question in the reason box.

4. Click **OK**.

This closes the dialog box.

To revoke hold status



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

1. Select the request you want with this status.

You will see a **Revoke hold status** button in the main content view on the **Information** tab. You can also see this status on the **Workflow** tab of a question was answered.

2. Click **Revoke hold status**.

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

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 more information about approval processes for IT Shop requests, see the Dell One Identity Manager IT Shop Administration Guide.

1. Click **My Actions | Pending requests**.

2. Mark the request you want to edit in the list of pending requests.

3. Select **Reroute approval** in the main content view.

This opens a dialog box, **Reroute Approval** showing approval levels and their approval steps.


4. Select one of the single approval steps shown and click **Reroute approval**.
5. Enter a reason for rerouting in the text box and click **Reroute approval**.

To delegate approval

1. Click **My Actions | Pending requests**.
2. Mark the request you want to edit in the list of pending requests.
3. Select **Delegate approval** under **more** in the main content view.
This displays the view **Select an employee who should approve instead**.
4. Select an employee from the list.

- OR -


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

 **NOTE:** For more information about using the filter function, see [Tips for using Web Portal](#) on page 14.

5. Click **Select** next to the employee you are looking for in the list of employees or in the result list, respectively.

This opens the dialog box **Enter the reason for adding an approver**.

6. Enter a reason for the delegation in **Reason**.
7. Click **Save** to delegate.
8. A message, saying that the delegation was sent, is displayed in **Pending Requests**.


 **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. Click **My Actions | Pending requests**.
2. Mark the request you want to edit in the list of pending requests.
3. Select **Add approver** under **more** in the main content view.
This shows the view **Choose an additional approver**.
4. Select an employee from the list.

- OR -

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

 **NOTE:** For more information about using the filter function, see [Tips for using Web Portal](#) on page 14.


5. Click **Select** next to the employee you are looking for in the list of employees or in the result list, respectively.

This opens the dialog box **Enter the reason for adding an approver**.

6. Enter the reason for another approver in **Reason**.


7. Click **Save** to enter the additional approver.

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

 **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.

Editing Pending Requests with the Chief Approval Team

If there are requests pending and the approver responsible is not available for some time 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 information, see the Dell One Identity Manager IT Shop Administration Guide.

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


To make approval decisions about escalated pending requests

1. Click **My Actions | IT Shop escalation**.
2. Mark the request you want to grant or deny approval for in the list of pending requests.
3. Enable **Approve** or **Deny** in the **Decision** column and click **Next**.

Some requests require more information before an approval decision can be made. In this case, you can view information about the pending request on the right-hand side of the main content in **Pending Requests**. The tab **Information** provides you with information about the product, recipient and requester, amongst others. Previously stored data is displayed under the product name in the list of pending requests. On the **Workflow** tab, you can see lifecycle of the request in chronological order. The **Compliance** tab shows you any rule violation for this request. For more information, see [Handling Requests when You Need More Information](#) on page 47.

- OR -

4. Click **Approve all** or **Deny all**.

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


5. Click **Next**.

This displays the **Approvals** view. In this view you see the request that you have marked.

6. Enter a reason for your decision in **Reason for approval** or **Reason for denial** or select a reason in **Standard reason** and click **Save approvals**.


Your reason helps provide an audit trail for requests

7. Enter the **Valid until expiry date** for the request if required.

 **NOTE:** This option is only available when approving a request.

8. Click **Save approvals**.

Answering Approval Inquiries

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


You may receive inquiries about requests. Inquiries are communications specific to a request. In the first view, you can see the employee and the inquiry. Using the **Plus** button you can get more information, for example, about the product/attestation procedure or edit status. You can see more information by clicking on the **information** button. If the inquiry is about an attestation procedure, you can see the page **Attestation policies** over the **Information** button. This gives you information about attestation procedures, approval policies and calculating schedules. For information on making inquiries, see [Handling Requests when You Need More Information](#) on page 47.

To answer an approval inquiry

1. Click **My Actions | Approval Inquiries**.
2. Click the desired inquiry, and click **Respond**.
3. Enter your response in **Your answer**.
4. Click **Save**.

Your answer is sent after confirming. Confirmation verification is displayed.

Viewing Approval History

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

In the approval history, you can view all products you have assigned, denied or canceled, or still being processed (status **Request**). The menu item corresponds to the information on offer in the menu item **Request History** in terms of structure and content. You can find information about functions and viewing options in **Tracking Requests**.


To use the advanced search function in the approval history

1. Click **My Action History | Approval History**.
This show the **Approval History** view.
2. Click **Advanced search**.
This displays more search settings in the **Approval History** view.
3. Change the name of the approver in the option **Approved by** if necessary.
4. Set the following search options:
 - a. Filter by request number: Enter the request number in the text box.
 - b. Request state: Enable one or more check boxes with different options to limit the search.
5. Click **Search**.

The search is carried out and all requests found taking the search settings into account are displayed in **Approval History**.

To cancel a delegation

1. Click **My Action History | Approval History**.
This shows all the products you have assigned, denied, canceled or edited.

 **NOTE:** To cancel a delegation, the product must have the status **Request**.

2. Mark a request you want to edit in the list.
3. Click **Withdraw request** in the main content.
4. Click **Withdraw delegation** in the dialog window.

You can only see this button if the approval has been delegated to someone else.

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

You can read about how you delegate approval for a pending request in [Granting or Denying Request Approval](#) on page 43.

To cancel additional approval

1. Click **My Action History | Approval History**.

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



NOTE: To withdraw an additional approval, the product must have the status **Request**. Once the additional approval has been canceled, you are the only approver for this procedure again and can add additional approvers.

2. Mark a request you want to edit in the list.
3. Click **Withdraw additional approval** in the dialog box.

You only see this button if other approvers have been added for this product.

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

You can read about how to add additional approvers in [Granting or Denying Request Approval](#) on page 43.

Requesting Email Notifications



NOTE: This function is only available if the Identity Management Base Module module is installed.

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**.
The view **My Settings** is displayed.
3. Select the **Mail Subscriptions** tab.
4. Click **Mail Subscriptions**.
5. Enable the **Receive email** check box next to the email notification you want to receive.
6. Click **Save**.

Delegating Roles

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

The menu item **Delegation** lists all direct and indirect roles, the associated role classes and your affiliation status to each role, for example, role supervisor. You have the option, to delegate one or more roles or roles in your area of responsibility.

Table 12: Delegation Status

Status	Description
Assigned	<p>This status is displayed for the current delegation.</p> <p>To end delegation before the given end date</p> <ol style="list-style-type: none">1. Click Delete.2. Click Yes to really cancel the delegation.
Approved	<p>You see this status if you have added a delegation for later use.</p> <p>To withdraw the delegation</p> <ol style="list-style-type: none">1. Click Withdraw.2. Confirm the security prompt with Yes.

To add a new delegation

1. Select **My Actions | Delegation**.
2. Enable the role you want **My Roles** in the column **Delegate**.

Roles that have already been delegated can be 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. Click **New Delegation**.

- OR -


Click **Delegate all my responsibilities** if you want to delegate all available roles to a particular person. This opens the dialog box **New delegation**.
4. Click **Assign** and select the employee you want to delegate.
5. Enter the period for the delegation in the date and time fields **Valid from** and **Valid til**.
6. Enable the option **Notify me if the recipient of the delegation makes a decision**.
7. Enable the option **The recipient can delegate this role**.
8. Enter a reason for the delegation in **Reason**.
9. Click **Save**.
10. Click **Yes** if you really want to delegate the selected role.

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. Select **My Actions | Delegation**.

The **Delegation** view is displayed.
2. Select the delegated role you want by checking the **Delegate** box.

 **NOTE:** You can recognize a delegation because the **[number] Delegations** is written in the role's **Delegated** column. You can only stop or withdraw delegated roles.

3. Select **Withdraw** or **Delete** in the main view.

If the delegation has already been approved it shows the status **Assigned** and can be deleted with **Delete**. If the delegation show the status **Request**, it has not yet been approved and can be canceled with **Withdraw**.

4. Click **Yes** to confirm.

Viewing your Delegation History

In the delegation history, you can view all the delegations you have issued. You can also see the employee you delegated for the task. For more information, see [My Action History](#) on page 84.

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 hardware or a workdesk associated with the problematic hardware, can play a part when adding a call.

To add a new call

1. Enter a detailed description of the problem in **Description**.
2. Select the product affected by the problem in **Product**.
You can see all possible products in the context menu.
3. Select the problem's rating in **Severity**.
4. Click the link **assign** next to **Cost center**.
This opens the dialog box **Cost center**.
5. Select an cost center from the list.
This closes the dialog box.
6. 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. Mark the call you want in the list.
More information about the call is displayed in the main content view. You can subsequently change **Severity**, **Description** and **Product** entries on the **Master Data** tab.
2. Select the **History** tab to view staff, status and implemented measures.

3. Select the **Attachments** tab to view any attachments.
4. Click **Save**.

Managing "My Responsibilities"

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


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

- employees
- Organizations
- business roles
- System Roles
- System entitlements
- other services
- file system
- Claim ownership


Working with Organizations

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 organization on the list, you may be able to:

- View a variety of information about the organization, including 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 86.
- Add members to the role. For details, see [Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services](#) on page 68.
- Add entitlements to the role. For details, see [Adding and Deleting Entitlements to Organizations, Business Roles and System Roles](#) on page 67.


 **NOTE:** As data owner, you can also access pending attestations for which you are the authorized approver, using the link [Click here to approve pending attestation cases](#) in the **Attestation** view.

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 see business roles for which you are responsible, view **Business Roles** in **My Responsibilities**.

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

- View a variety of information about the business role, including an overview, its members, entitlements, associated risks and attestation cases, rule violations and usage. For more information, see [Description of Commonly Used Tabs in Views](#) on page 86.
- 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 69.
- Add members to the role. For details, see [Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services](#) on page 68.
- Add entitlements to the role. For more information, see [Managing "My Responsibilities"](#) on page 56.

To add a new business role

1. Click **My Responsibilities | Business Roles**.


The **Business Roles** view displays a list of business roles for which you are responsible.

2. Click **New business role**.

This opens the **Create a new business role** view.

3. Enter a unique name for the business role in the **Business Role** text box.
4. Click **Assign** next to the **Role class** text box and select the role class.
5. Enable the box **Employees do not inherit** if required.
6. Enter a detailed description of the business role in the **Description** text box.
7. Enter additional information about the business role in **Commentary** if required.
8. Click **Save** to create the business role.

The business role is shown to the business role manager.

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

To add a new system role

1. Click **My Responsibilities | System Roles**.

The **System Roles** view displays a list of system roles for which you are responsible.

2. Click **New system role**.

This displays the **New System Role** view.

3. Enter a unique name for the business role in the **System Role** text box.
4. the Enable box to allow the system rolIT ShopIT Shope to be requested through the .
If this option is enabled, the system role can assigned directly to employees or roles.


- OR -

Enable the **Only use in IT ShopIT Shop** check box to allow the role to be requested by, but not directly assigned to employees.

If this option is enabled, the system role can assigned directly to employees or roles.


5. Click **Save** to create the system role.

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
- Notes groups
- SAP groups
- SAP structural profiles
- SharePoint® groups
- SharePoint®
- Oracle E-Business Suite
- UNS

 **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 hyperview), its members, attestation cases and usage of the different role classes. For more information, see [Description of Commonly Used Tabs in Views](#) on page 86.
- 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 69.
- Add members to system entitlements. For details, see [Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services](#) on page 68.
- Obtain an overview of all group which are members of a system entitlement.


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. Click **My Responsibilities | System Entitlements**.


The **System Entitlement** view displays a list of system roles for which you are responsible.

2. Select the Active Directory® group you want from the list of system entitlements.
3. Select the **Owners** tab for the selected Active Directory® group.

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

4. Click **Create new owner role**.
This opens the **Create new owner role** dialog box.
5. Enter the name of the new owner role in **Application role** and a description in the respective text box.
6. Click **Save**.


The dialog box is closed and the new owner role is displayed next to **Product owner** on the **Owner** tab.

 **NOTE:** After you have added a new owner role, you must assign the product owner you want to this role.

7. Click **Assign** next to **Product owner**.
This show the **Product owner** dialog box
.
8. Click the **Product owner** link and select the new owner role if it is not already preselected.
The dialog box is closed and any changes made are marked next to **Product owner**.
9. Click in the **Available** section, the name of the employee you want in the in the list (multi-select is possible).


The icon next to the name of the selected employee in the **Available** section changes and is added to the **Assigned** section.

10. Click **Save**.

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


To assign an attestor to a Active Directory® group

1. Click **My Responsibilities | System Entitlements**.
The **System Entitlement** view displays a list of system roles for which you are responsible.
2. Select the Active Directory® group you want from the list of system entitlements.
3. Select the **Attestors** tab for the selected Active Directory® group.

 **NOTE:** Before you can assign a new attestor, you must add a new attestor role for this employee.

4. Click **Create new attestor role**.
This opens the **Create new attestor role** dialog box.
5. Enter the name of the new attestation role in **Application role** and a description.
6. Click **Save**.

The dialog box is closed and the new owner role is displayed next to **Attestor** on the **Attestors** tab.

 **NOTE:** After you have added a new attestor role, you must assign the attestor you want to this role.

7. Click **Assign** next to **Attestor**.
This opens the dialog box **Attestors**.
8. Click the **Attestor** link and select the new attestor role if it is not already preselected.
The dialog box is closed and any changes made are marked next to **Attestor**.
9. Click in the **Available** section, the name of the employee you want in the in the list (multi-select is possible).
The icon next to the name of the selected employee in the **Available** section changes and is added to the **Assigned** section.
10. Click **Save**.


To edit requestability settings of system entitlements

1. Click **My Responsibilities | System Entitlements**.
The **System Entitlement** view displays a list of system roles for which you are responsible.
2. Select the system entitlement you want from the list.
3. Select the **Master Data** tab and enable and set one or more of the IT Shop check boxes.
For more detailed information about requestability of service items, see the Dell One Identity Manager IT Shop Administration Guide.
4. Click **Save**.

To add a new group membership

1. Click **My Responsibilities | System Entitlements**.
The **System Entitlement** view displays a list of system roles for which you are responsible.
2. Click the system entitlement and click the **Child groups** tab.
3. Click the **New child group** button.
4. Click **Assign** and choose the group you want.
5. Click **Save** to assign the group.

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. Click **My Responsibilities | System Entitlements**.
The **System Entitlement** view displays a list of system roles for which you are responsible.
2. Click the desired system entitlement managed by an Active Roles Server and select the **Master data** tab.
3. To edit the group, make the following check box setting:
 - 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. Click **Add account**, if you want to add other owners.
- OR -
Click on **Add group** to add more groups.
5. Click **Save**.

To delete a group membership

1. Click **My Responsibilities | System Entitlements**.
The **System Entitlement** view displays a list of system roles for which you are responsible.
2. Click the system entitlement and click the **Child groups** tab.
3. Enable the check box for the group to remove.
4. Click **Remove selected**.

To view access permission for an Active Directory® and a SharePoint® group

1. Click **My Responsibilities | System Entitlements**.
The **System Entitlement** view displays a list of system roles for which you are responsible.
2. Click the system entitlement you want and select the **Access** tab.
3. Click the plus sign next to the group to extend the list and view parent groups.

 **NOTE:** If more parent groups are shown with a plus sign, click on it until either a folder or a file is shown. This means you can also view access permissions for parent groups.

A check marks are displayed in the columns **Read**, **Write** of the select system entitlement and a button in the **Details** column. Read/write access is given to the file or folder depending on the columns in which these check marks are show.

4. Select **Details** next to the file or folder.
This opens the dialog box **Access Control List** showing the assigned permissions.

To assign a hardware object to a Active Directory® group

1. Click **My Responsibilities | System Entitlements**.
The **System Entitlement** view displays a list of system roles for which you are responsible.
2. Click the system entitlement you want and select the **Memberships** tab.
Two tabs are shown in this view.
3. Click the tab **Active Directory® computers**.
4. Click **Assign** next to the Active Directory® computer
The **Assign** view is displayed. This view is divided into two sections. In the first section, **Available**, you can select objects. The **Assigned** section lists selected objects.
5. Select the object you want and click **OK**.
The view is closed and the selected object is displayed next to Active Directory® computers.
6. Click **Save**.

To view details of an entitlement assignment to a specific member

1. Click **My Responsibilities | System Entitlements**.

The **System Entitlement** view displays a list of system roles for which you are responsible.

2. Click the system entitlement you want and select the **Memberships** tab.

Two tabs are shown in this view.

3. Click the **Employees** tab.


A list of members appears.

4. Mark the member you want.

5. Click the arrow next to **Analysis for**

More entries are displayed. Like, the origin of the entitlement and related details.

Working with File System and SharePoint® Resources

 **NOTE:** This function is only available when the module Data Governance Module is installed.

Under the menu items **File System** and **SharePoint®**, you can see different file systems and **SharePoint®** resources. You may be responsible for folders, shares or files, as well as **SharePoint®** resources at site level and below. If you do not think you should be the owner of a resource, you can reject or change the ownership. You can get an overview of everything below.

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

- View a hyperview of a resource with its necessary details. For more information, see [Description of Commonly Used Tabs in Views](#) on page 86.
- Change the properties of the resource. For more information, see [Editing Master Data of Business Roles, System Roles and other Services](#) on page 69.
- View the activity on the resource in the last 7 days.
- View accounts and groups that have access to the resource. Request modification of access rights.
- View different lists of historical changes to properties, taxonomies and objects linked to resources. For more information, see [Description of Commonly Used Tabs in Views](#) on page 86.

NOTE: You can only see the **History**, **Attestation** and **Access** tabs if you are a business owner, compliance officer or auditor.

- Generate reports for the resource.
- View a risk analysis about a resource. For more information, see [Description of Commonly Used Tabs in Views](#) on page 86.
- View attestation cases. For more information, see [Description of Commonly Used Tabs in Views](#) on page 86.

Table 13: List of Governed Data Reports

report	Description
Data Owners vs. Perceived Owners	Displays all the resource data owners who have had resource access. The perceived owners are displayed for the resource in percent as well as the business owner.
Data Ownership Over Time	Understand how ownership of resources changes over time for better control over access to data.
Perceived Owners for Data Under Governance	<p>Perceived ownership is estimated based on folders with a high level of activity and based on accounts with the highest percentage of weighted activity. Actions such as writes and creates are weighted heavier than reads. This excludes resources that have a business owner already assigned.</p> <p>Historical resource activity is used to determine the perceived owner and provide guidance on who should be assigned as the business owner for a particular resource. For details on assigning business owners, see the Data Governance User Guide.</p>
Resource Access	<p>This report identifies which accounts have access to the resource. This can help you meet your compliance and audit goals by ensuring only authorized users can access the specific resources.</p> <p>The report includes subfolders and files of the identified resources if the security differs from the parent (for example, if inheritance is overridden or blocked).</p> <p>This report helps to identify data with several access points that should be monitored and potentially governed. Content that is available to “Everyone” or “All Sales” for example, can pose a high risk of having a sensitive file placed within it. These entitlements might arise either in error or through malicious intent.</p>
Resource Activity	Provides a list of activities recorded over a period of time to verify proper resource usage and make decisions on removing access for particular accounts.
Resources without ownership	This report shows data with heavy activity but without an owner. The report contains the perceived owner for this resource.

To generate a report for a resource

1. Select **My Responsibilities | File system**
- OR -
Select **My Responsibilities |SharePoint@**.
2. Select the resource on the **My Actions** or **All my resources** tab.
3. Click the **Reports** tab.
4. Select the desired report, and click **Generate Report**.
This opens a dialog box.
5. Click **Send report**.
The report will be delivered to your email account.

To change the access permissions for a resource

1. Select **My Responsibilities | File system**.
- OR -
Select **My Responsibilities |SharePoint@**.
2. Select the resource on the **My Actions** or **All my resources** tab.
3. Click the tab **Access**.
4. Click **Request modification**.
This opens the dialog box **Modifying Access**.
5. Enter a reason for the modification in the text box.
6. Click **Send**.
The the request is sent immediately and not added to the cart.

To reject the ownership of a resource

1. Select **My Responsibilities | File system**.
- OR -
Select **My Responsibilities |SharePoint@**.
2. Select **All my resources**.
3. Click the resource you want, and then select **Master Data**.
4. Click **Reject ownership**.
This opens the dialog box **Reject ownership**.
5. Enter a reason in the text box if you want to make a correction.
6. Click **Send**.
For more information, see [Using your Shopping Cart to Submit your Requests](#) on page 37.

To make an item available for request in the

1. Select **My Responsibilities | File system**.
- OR -
Select **My Responsibilities |SharePoint@**.
2. Select the tab **All my resources**.
A list of resources under your ownership is displayed.
3. Click the resource you want, and then select **Master Data**.
4. Enable the **Available in IT Shop** check box.
This resource can now be requested by other users.
5. Click **Save**.


To view groups and account with access permissions for a governed resource and to request a change if necessary

1. Select **My Responsibilities | File system**.
- OR -
Select **My Responsibilities |SharePoint@**.
2. Select the tab **All my resources**.
A list of resources under your ownership is displayed.
3. Click the resource you want, and then select **Access**.
4. Click the radio button **Assigned permissions**.
All Active Directory® groups and accounts are displayed that have at least one of the five access types to the resource. If the assigned permissions are not correct, you request a change to the access permissions.
5. Click **Request modification**, if you want to correct the access rights.
This opens the dialog box **Modifying Access**.
6. Enter a reason for the change in the text box and click **Send**.
The system administrator assigns the access types to a resource. The system administrator makes the modification.

To view access permissions of authorized accounts and groups

1. Select **My Responsibilities | File system**.
- OR -
Select **My Responsibilities |SharePoint@**.
2. Select the tab **All my resources**.
A list of resources under your ownership is displayed.
3. Click the resource you want.
4. Click an account or group in the **Accounts with permissions** shape on the **Overview** tab.
A new page with the selected account is opened.
5. Select the tab **Access**.
This displays all governed data with access to the account.

Managing other Services

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

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 (hyperview) with all details about memberships, attestation cases and usage. For more information, see [Description of Commonly Used Tabs in Views](#) on page 86.

- Change resource properties. For more information, see [Editing Master Data of Business Roles, System Roles and other Services](#) on page 69.
- 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 69.


To add a new application

1. Select **My Responsibilities | Other Services**.
2. Click **New application**.
This displays the **New Application** view.
3. Edit the options in the view and click **Save**.

To add a new resource

1. Select **My Responsibilities | Other Services**.
2. Click **New resource**.
This displays the **New Resource** view.
3. Edit the options in the view and click **Save**.


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. No one has claimed ownership of the listed groups and authorized users can do so. 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. Select **My Responsibilities | Claim Ownership**.
This shows the **Claim Ownership** view.
2. Click **Assign**.
This shows the **Select a group** view.
3. Select the group you want from the list in the **Select a group** dialog box.
The dialog box is closed and the group is displayed in the **Claim Ownership** view with more details.


 **NOTE:** If you want to claim ownership for more groups, click **Claim Ownership** in the **Claim Ownership** view.

4. Click the **Claim Ownership** button.
Your settings are saved.

To change you ownership group


1. Click **Change** in the **Claim Ownership** view.
This shows the **Select a group** view and you can claim ownership for another group of your choice.
2. Select the group you want in the dialog box **Select a group**.
The dialog box is closed and the group is displayed in the **Claim Ownership** view with more details.
3. Click the **Claim Ownership** button.
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 that an employee can gain entitlements:

- Directly, 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. Select **My Responsibilities | Organizations**, if you want to assign an entitlement to a department, cost center or location and click on the organization you want.
- OR -
Select **My Responsibilities | Business Roles**, if you want to assign an entitlement to a business role and click on the business role you want.
- OR -
Select **My Responsibilities | System Roles**, if you want to assign an entitlement to a system role and click on the system role you want.
2. Select the **Entitlements** tab.
Available entitlements are displayed in a list.
3. Click **Add a new entitlement**.
This opens the dialog box **Add a new entitlement**.
4. Click **Assign** next to **Entitlement type**.
This opens the dialog box **Entitlement type**.

5. Select the entitlement you want from the list.
This closes the dialog box. This opens the dialog box **Add a new entitlement** showing the selected entitlement.
6. Click **Assign** next to **Entitlement**.
This opens the dialog box **Entitlement** with a list of entitlements.
7. Select the entitlement you want.
This closes the dialog box. This opens the dialog box **Add a new entitlement** showing the selected entitlement.
8. Click **OK**.
Your cart appears. For more information, see [Using your Shopping Cart to Submit your Requests](#) on page 37.

To delete an entitlement

1. Select **My Responsibilities | Organization**, then select the desired department, cost center or location from which to delete the entitlement.
- OR -
Select **My Responsibilities | Business Roles**, to delete an entitlement from a business role.
- OR -
Select **My Responsibilities | System Roles**, to delete an entitlement from a system role.
2. Click the **Entitlements** tab.
Available entitlements are displayed in a list.
3. Enable the check box next to the entitlement (multi-select is possible) you want to delete.
4. Click **Delete entitlement**.

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 a new membership

1. Select **My Responsibilities | Organizations**, if you want to assign employees to an organization and click on the organization you want.
- OR -

Select **My Responsibilities | Business Roles**, if you want to assign employees to a business role and click on the business role you want.

- OR -

Select **My Responsibilities | System Roles**, if you want to assign employees to a system role and click on the system role you want.

2. Select the **Memberships** tab.

This displays a list of employees with access rights.

3. Click **Request memberships**.

The **Request memberships** dialog box opens with a list of employees in alphabetical order. This view is divided into two sections. In the **Online** section is a list of users for you to select from. Select users are listed in the section **Up to date**.

4. Select the employee you want from the list by clicking on it (multi-select is possible).

The selected users are moved to **Up to date**. In **Available** section, the icon next to the user changes.

5. Click **Add to cart**.

Your cart appears. For more information, see [Using your Shopping Cart to Submit your Requests](#) on page 37.

To delete a membership

1. Select **My Responsibilities | Organization**, if you want to remove a membership from an organization and click on the organization you want.

- OR -

Select **My Responsibilities | Business Roles**, if you want to remove a membership from a business role and click on the business role you want.

- OR -

Select **My Responsibilities | System Roles**, if you want to remove a membership from a system role and click on the system role you want.

2. Select the **Memberships** tab.

This displays a list of employees with access rights.

3. Enable the check box next to the employee (multi-select is possible) you want to delete.

4. Click **Delete memberships**.

Your cart appears. For more information, see [Using your Shopping Cart to Submit your Requests](#) on page 37.

Editing Master Data of Business Roles, System Roles and other Services



NOTE: This function is available if the Business Roles Module or System Roles Module 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. Select a submenu under **My Responsibilities** to specify the type of responsibility you want (organization, business role or other).
2. Click the desired entry in the view of the selected submenu.
3. Select the tab **Master data**.
4. Make your changes.
5. Click **Save**.

Saving the changes may take a few minutes.

Adding Tags for Service Items


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

You can add tags if you are the product owner and the service item can be requested in the IT Shop. Tags help the 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 28 or in the IT Shop guide. You can add tags in the IT Shop (for more information, see the Dell One Identity Manager IT Shop Administration Guide) as well as in the Web Portal. Add tags in the Web Portal as a product owner.

To add a tag for a service item

1. Select a submenu in **My Responsibilities**, containing the object to which you want to assign a new tag.
The selected object is displayed in a new overview.
2. Click the object names.
A new page is opened showing the objects.
3. Select the tab **Overview** and click the object name for which you want to add the tag in the **service item** shape.
A new page opens showing this object.
4. Select the **Tags** tag and click **New tag**.
This opens the dialog box **Create a new tag**.
5. Enter the tag you want in **Change label**.
Enter additional information about the tag in **Description**.
6. Click **Save**.
You can add more tags for the object.


Adding and Editing Employees

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


You can add new employees to the system using this menu item. This function is main used for adding external people, for example, you may need to set up a sub-contractor. If you add an employee who already exists, the data is either completely transferred to the database or the previously entered data will be updated and/or amended depending on system configuration and settings of imports from the connected systems.

To add a new employee


1. Click **My Responsibilities | People**.
This opens the **People** view with a list of employees.
2. Click **Add a new employee** at the bottom of the view.
This opens the **Add a New Employee** view.
3. Enter information in text and option fields.
You must enter information in all field marked with an asterisk *.
4. Click **Save** to save the new employee.
5. Confirm the security prompt with **Yes**.

 **NOTE:** When you save the employee, the system checks to ensure you have entered a unique first/last name combination. If any employees with the same name already exist, they are displayed. If you want to add the employee, accept by clicking **Yes**. Click **No** to cancel.

To view and edit employee data

1. Click **My Responsibilities | People**.
This opens the **People** view with a list of employees.
 **NOTE:** There is a filter to help you search for a particular employee.
2. Click **Select** next to the employee you have chosen.
3. Change or extend the employee data in the **Master Data** tab and click **Save**.
The tabs **Overview**, **Requests**, **Risk** and **History** are identical to the those in the **Audit | Employee Details** menu, For more information, see [Auditing - Employee Details](#) on page 92.


To view and edit employee memberships

1. Click **My Responsibilities | People**.
This opens the **People** view with a list of employees.
 **NOTE:** There is a filter to help you search for a particular employee.
2. Click **Select** next to the employee you have chosen.
3. Click the **Entitlements** tab to view assigned entitlements and memberships.
4. Select **Edit memberships** to view memberships of the selected employee.
A table is displayed with the employee's memberships and the membership object types.
5. Mark the membership whose details you want view in the main content view.
6. Enable the check box next to the membership if you want to delete it.
7. Click **Delete Membership**.

To view and edit employee delegations


1. Click **My Responsibilities | People**.

This opens the **People** view with a list of employees.

 **NOTE:** There is a filter to help you search for a particular employee.

2. Click **Select** next to the employee you have chosen.
3. Click the **Entitlements** tab to view assigned entitlements and memberships.
4. Select **Edit delegations** to view a table with roles, which are not delegated.
5. Enable the check box for the role you want to delegate to the employee.

This displays details of the role in the main 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.

6. Click **New delegation**.


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

7. Enter the required information in text and option fields and click **Save**.

To view employee entitlements and memberships at a glance

1. Click **My Responsibilities | People**.

This opens the **People** view with a list of employees.


 **NOTE:** There is a filter to help you search for a particular employee.

2. Click **Select** next to the employee you have chosen.
3. Click the **Entitlements** tab to view assigned entitlements and memberships.
4. Select the **Overview** tab to view all memberships and entitlements at a glance.

To view an employee's risk index

1. Click **My Responsibilities | People**.

This opens the **People** view with a list of employees.

 **NOTE:** There is a filter to help you search for a particular employee.

2. Click **Select** next to the employee you have chosen.
3. Click **Risk** to view the risk index analysis.
4. Click **Risk index functions**, if you want to view attributes and assignments in more detail.

The Risk Assessment view is displayed. This view is divided into two parts, **Attribute-based calculation** and **Assignment-based calculation**. These attributes and assignments are listed individually and displayed with values **Weighting / change value**, **Calculation type** and **Result value**.


5. Click **Close**.

To view details of an entitlement assignment to a specific employee

1. Click **My Responsibilities | People**.

This opens the **People** view with a list of employees.

2. Click the employee you want, and then select **Entitlements**.

 **NOTE:** The option **Edit memberships** must be set.

3. Mark the entitlement you want.
4. Click the arrow next to **Analysis for ...**

More entries are displayed. Like, the origin of the entitlement and related details.

To view details of a resource access assignment to a specific employee

1. Click **My Responsibilities | People**.

This opens the **People** view with a list of employees.

2. Click the employee you want, and then select **Resource Access**.

Two tabs are shown in this view.

3. Click the **Resources** tab.

This displays a list of resources.

4. Mark a resource.
5. Click the arrow next to **Analysis for ...**

More entries are displayed. Like, the origin of the entitlement and related details.

To view details of pending attestation cases for a specific employee

1. Click **My Responsibilities | People**.

This opens the **People** view with a list of employees.

2. Click the employee you want, and then select **Attestation**.

Four tabs are shown in this 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.

More details about the case are displayed in the main content view. You can approve the attestation case if you have the necessary permissions. You can, however, also show other approvers for pending attestation cases or send a reminder to the approver.

To assign an employee to a new manager

1. Click **My Responsibilities | People**.

This opens the **People** view with a list of employees.

2. Click the employee you want to view.

This open the **Master data** view.

3. Click **Assign to new manager**.

This opens the **Assign to New Manager** view


4. Click **Assign** next to **New manager**.

This opens the dialog box **New manager** with a list of employees.

5. Select the employee you want to assign as manager from the list.

The dialog box closes and you are returned to the **Assign to New Manager** view.


6. Enable the check box **Effective date** and set the time and date from which the new manager takes effect.
7. Click **Submit** after you have set everything as required.

 **NOTE:** You can cancel requests that have already been approved for the employee who has just been assigned a new manager. In this case, disable the check box in the column **Cancel on the effective date**.


This opens the **Assign to New Manager** dialog box.

8. 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 for a change of manager is displayed in the menu **My Actions | Pending Requests** of the approvers authorized to grant or deny approval.

Accessing Other Applications

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

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

- Click the **Applications** menu and choose the desired web application.

The application may appear within the Manager, 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. Your 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.

- [Discovering your Statistics on the Start Page](#)
- [Using Views to Get Information](#)
- [Generating Reports](#)

Searching in the Web Portal

You can run a context independent search in the Web Portal based on the following search criteria:

- All requestable products
- By tag
- Your staff
- Your business roles, resources, system roles and system entitlements
- Your cost centers, departments and locations
- Your requests
- Your governed data
- If you are a security officer, all your confirmed policies
- If you are a compliance officer, all your compliance rules

To run a search in the Web Portal

1. Enter the term or part of a term to search for in **Search**.
2. Click the **Search** or press **Enter**.
3. Select the object you want from the result list (employee, product or cost center).

- OR -

Use the sort or filter function to refine the search.

For more information, see [Tips for using Web Portal](#) on page 14.

Once you have made a selection, you can continue.

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

1. Click the arrow next to the info icon in the Web Portal header.
This opens a menu with other menu items.
2. Select **Help** in the menu.
The Dell One Identity Manager Web Portal User Guide is opened as online help.

Information about the Current Connection

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

 **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 the arrow next to the info icon in the Web Portal header.
This opens a menu with other menu items.
 **NOTE:** You find the menu item **Properties** in the mobile view.
2. Select **Connection**.
This opens the dialog box **Connection**.
3. Select the tab for the information type you want to view in more detail.

Discovering your Statistics on the Start Page









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

In the <Info System> you will find 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 the arrow button on the right to "leaf" through all available statistics in each section. For more information, see [What Statistics are Available?](#) on page 80.

Statistics

Graphical representation of data is depicted through various types of diagram. Heatmaps also provide data in graphical form. However, these are described in a separate chapter.


Table 14: 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 statistic.
	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.
	This arrow icon shows the value has decreased 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 decreased 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

1. Select either **My Identity** or **Access Governance** in the main section on the start page.
All the organizational units for which you are responsible are displayed on the start page. This units are divided into their associated subgroups.
2. Click the desired organizational unit 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, organizational units, which take you to a page with source data.


To view data from an organization unit

 **NOTE:** You can only view source data for certain organizations. You can view a heatmap or statistics, with graphical representation, for certain organizational units.

1. Select either **My Identity** or **Access Governance** in the main section on the start page.
All the organizational units for which you are responsible are displayed on the start page. This units are divided into their associated subgroups.
2. Click the organizational unit you want to view in more detail, for example, employees without user accounts or departments without managers.
This displays a view with the corresponding data.


To customize the information displayed on a statistics view

- Click the filter icon in the column you want in your selected statistic's view.
This opens a dialog box for the selected filter. For more information, see [Tips for using Web Portal](#) on page 14.

 **NOTE:** The filter function is not available for all statistics.

Heatmap

The heatmap in the Web Portal presents organizational units 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 organizational unit. For example, the more employees an organizational unit has, the larger the rectangle in the view.

 **NOTE:** You can see an overview of the organizational units you are responsible for, in the main section **My Identity** or **Access Governance**.


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. Yellow is in the middle of the scale and represents the average, which may mean there have been no changes experienced by the organizational unit since the last evaluation. 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 following risky results or properties in a heatmap:


- Policy violations
- Average number of permissions per employee
- Highest employee risk index by

- Average employee risk index by
- Policy violations by
- Compliance rule violations by
- Highest resource risk index by host

To view data from an organizational unit

 **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 organizational unit 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 to suit your own requirements. The settings **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**.


Your 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 on 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 organizational units

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.

 **TIP:** You also obtain additional information about the organizational unit of your 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. Click on one of the clickable items to obtain more information.

- OR -

Click the link **Display object details** to obtain more information.

A view with detailed information, spread over several tabs, is displayed for the square you click on.

What Statistics are Available?

The statistics you see in the Web Portal depend on your roles and permissions. Only statistics relevant to you are available on the start page of the mail section **My Identity** and **Access Governance**. Statistics can be customized to display the objects and statistics that interest you. For more information, see [Discovering your Statistics on the Start Page](#) on page 77. You can also sort and filter statistic information, and export any table to a report. For more information, see [Discovering your Statistics on the Start Page](#) on page 77.

High Risk Overview

You will find an overview of critical objects in the **Access Governance** in the menu **Compliance**. The view lists critical objects and divides them into different groups. Each group shows you 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. You can see the following in the <High risk overview> in the statistics: You can view the following information in **High Risk Overview**:

- 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. There are statistics for the following themes:

- rule violation
- Policy violations
- Compliance violations
- Compliance status
- Rule status
- Employee by risk index

Use the appropriate tab to select the following information:

- Departments
- Compliance Frameworks
- Global statistics
- Employees
- Rule groups
- Rules
- Policy groups

For more information, see [Working with Compliance](#) on page 102.

Risk

For more information about this subject, see [Main Content Page](#) on page 11. The following statistics can be displayed in this view.

- Number of active employees with a risk index of more than 0.5
- Highest risk index of all employee per department, location, cost center
- Average risk index of employees
- Employee by risk index
- Average risk index of employees

Policies

For more information about this subject, see [Main Content Page](#) on page 11. The following statistics can be displayed in this view.

- Policy violations (actual)
- Pending policy violations
- Overdue policy violations
- Policy violation per department, location, cost center
- New policy violations
- Policy violations (7 days)
- Policy violation approval rates
- Policy violation approval rates

Organizations

The **Organization** area shows you the following statistics for departments under your management:

- Information about employee accounts
- Information about employees
- rule violation
- Information about pending requests
- The top roles and entitlements

For more information, see [Working with Organizations](#) on page 56.

IT Shop

The shop is the mechanism employees use to make requests. You can use statistics in IT Shop on the start page to track:

- Which products are the most popular, both by product owner and by shop
- How fast requests are processed
- Request frequency over time

For more information, see [Working with Organizations](#) on page 56.

attestation

For more information about this subject, see [Main Content Page](#) on page 11. The following statistics can be displayed in this view.

- Pending attestation cases
- Overdue attestations
- Pending attestation cases
- Attestation approval rates
- Attestation decisions
- Attestation status by type
- attestation

target system

For more information about this subject, see [Main Content Page](#) on page 11. The following statistics can be displayed in this view.

- Employees without user accounts
- Entitlements without requests (AD)
- User accounts without requests
- Pending membership attestations per
- Number of user accounts with a risk index of more than 0.5
- Number of entitlements with a risk index of more than 0.5
- User accounts with a risk index of more than
- Entitlements with a risk index of more than
- Groups with / without user account assignments
- Entitlements without requests (EBS), (LDAP), (SAP R/3), (Sharepoint)
- Disabled employees with enabled user accounts
- Locked user accounts of enabled employees (AD), (EBS), (LDAP), (SAP R/3)
- Role with/without user account assignments

Governed Data



NOTE: This function is only available when the module Data Governance Module is installed.

Governing unstructured data allows for better management, including controlling the access to data, increased self-sufficiency for managers, and better data integrity. By its nature, governed data has value to your company. **Governed data** statistics on the start page provide an overview of:

- Most active resources
- Employees who have the most activity on governed resources
- Proportion of governed resources that have related policies
- Number of resources that are governed, owned, or published in a given time frame
- Summary of the governed resources

Detailed information about this topic

- [Working with File System and SharePoint® Resources](#)
- [Assigning Resource Owners](#)

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. You can view:

- Information about You and Your History
- My Business Ownerships
- Auditing Information

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 Web Portal](#) on page 14. Many views share common pages. For more information, see [Description of Commonly Used Tabs in Views](#) on page 86.


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 hyperview 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 hyperview, 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

1. Click the arrow next to the current user in the header and select **My Profile**.
The **Overview** is displayed in a hyperview.

2. Move the shapes if you want to improve the overview to better view the details.

 **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 8 and [Using the White Pages to Look Up Employees](#) on page 85.

To open the "Contact Data" view

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

This opens a menu with other menu items.

2. Select **My Settings**.

The tab **Contact Data** is pre-selected and is 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 26.
- Approvals and denials of employees' requests
For more information, see [Editing Pending Violations](#) on page 116.
- Attestation decisions
- Rule violation decisions
- Policy violations you have edited
- Roles you have delegated to employees
For more information, see [Delegating Roles](#) on page 53.

To view your action history


1. Click **My Action History**.
2. Select the submenu of actions you want to review.

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 Web Portal](#) on page 14.

4. Click on the available links to display more details.

Using the White Pages to Look Up Employees

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


The **White pages** list 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 Web Portal](#) on page 14.

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 the arrow next to the info icon in the Web Portal header.
This opens a menu with other menu items.
2. Select **White pages** from the menu.
3. Search for the employee.
For more information, see [Tips for using Web Portal](#) on page 14.
4. Click **Information** for more details, for example, the default email address.

My Responsibilities

 **NOTE:** This function is available if the Identity Management Base Module module is installed.

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
- file system
- SharePoint®
- other services


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 Web Portal](#) on page 14. For information about managing business ownerships, see [Managing "My Responsibilities"](#) on page 56.

To view information about your business ownerships

1. Click **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 86.

Auditing

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


If you are a manager or auditor, you may have access to the **Auditing** menu. The **Auditing** menu gives you an overview of all items for which you are responsible. You will find this menu in the section **Access Governance**. You can use it to check that policies are being properly followed by employees. 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 Web Portal](#) on page 14. For more information on **Auditing**, see [Auditing Activity and Managing Compliance](#) on page 92.

To view auditing information

1. Select the menu **Auditing**.
2. Select a menu 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 on the tables, see [Description of Commonly Used Tabs in Views](#) on page 86.

Description of Commonly Used Tabs in Views

 **NOTE:** This function is only available when the module Identity Management Base Module is installed.

Some views have multiple tabs to provide you with all of the information. 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 Web Portal](#) on page 14.

Attestation

 **NOTE:** This function is only available when the module Attestation Module is installed.

The **Attestation** page shows you a list of attestation cases. For each case you can see the current status and the creation date in the main detailed view. You can:

- 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 main detailed view.
- You can view approvers for pending attestation cases.

Compliance



NOTE: This function is only available when the module Compliance Rules Module is installed.

The **Compliance** page shows you existing rule violations. If there are rule violations for your selected item, a warning appears. Click the **Compliance** tab to view information about the rules that have been violated, the entitlements involved, and the risk index. Mark one of the compliance violations in the list to view more detailed information about the violation in the main view. For information about compliance, see [Working with Compliance](#) on page 102.

Entitlements

The **Entitlements** overview provides you with a list of entitlements assigned to the selected item. Mark one of the **Entitlement** violations in the list to view more detailed information about the violation in the main view. For information on adding new entitlements, see [Adding and Deleting Entitlements to Organizations, Business Roles and System Roles](#) on page 67.

History

You can use the **History** overview to see changes to an item over time. It lists all changes, statuses and comparisons of properties, memberships, entitlements, rule violations and taxonomies for your chosen time period. The overview is divided into 3 sections **Property changes**, **Memberships changes** and **Entitlement changes**. Use the arrow next to each section to expand the hidden list with corresponding entries. You can choose the version of the view that is most helpful:

- Change log
This is the first view shown when you open the **History** page. Use the dates fields to select the time period to examine.
- State overview
Shows a list of all modified properties (for example, changes to last name or department) with the value and validity period.
- State comparison
Lists the current properties, memberships, business ownerships and rule violations, and allows you to compare to the value on the current or a historical date. You can either choose a date from the menu, or scroll through the available change dates using the **Previous** and **Next** buttons.

Master Data

In the Manager, master data is the information that has been entered about an item. You can use this to see the properties, or, if you have access, you can edit the item. Make any changes, and then click **Save**.



NOTE: Many items have a risk index as one of the properties. For information about risk indexes and how they are used, see the Identity Management documentation.

Memberships

The membership overview provides you with a summary of all employees that have access to the selected item. Mark an employee in **Memberships** to view more detailed information in main view. For more information about requesting and deleting memberships, see [Requesting and Deleting Memberships to Organizations, Business Roles or System Roles, System Entitlements and Other Services](#) on page 68.

Overview

The overview is a hyperview. The center of the hyperview 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. For more information about hyperviews, see [Tips for using Web Portal](#) on page 14.

Risk

Many items have a risk index associated with them, allowing the Manager 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 on configuring risk index functions, see [Modifying Risk Calculators](#) on page 105.

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 within. 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 symbol

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** page.
2. Select a role in the hierarchy.
3. Select a subrole by clicking on the name of the role in the chart.
- OR -
4. To move up through the hierarchy, Click the back arrow next to the top of the chart.
- OR -
5. Click **Information** to see the assigned employees.



NOTE: Click **More information** to get more information about the chart and its elements.


To analyze governed data access

1. Select the **My Responsibilities | File system**.
The view **File system** is displayed. The tab **My resources** is preselected.
2. Select the resource you want to analyze in **My resource**.

The resource is shown with more tabs.

3. Select **Usage**.
4. Select one of the following options:
 - a. Display employees with access to this resource.
This shows all employees who are entitled to access this resource. And the employees that do not have access to the resource despite their permissions.
 - b. Display employees who have accessed this resource in the past 7 days.
This only takes into account employees who have accessed the resource in the past 7 days, not depending on whether these employees had access to the resource.
5. Select a role in the hierarchy.
6. Select a subrole by clicking on the name of the role in the chart.
- OR -
7. To move up through the hierarchy, Click the back arrow next to the top of the chart.
- OR -
8. Click **Information** to see the assigned employees.

Generating Reports

 **NOTE:** This function is only available when the module Report Subscription Module is installed.

Reports are created in the Report Editor. 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.


Report Subscriptions

The **Report subscriptions** menu item is divided into three sections:

- Available reports
Lists all the reports to which you can subscribe. You can see a description of each report. You can subscribe to a report using **Subscribe**.
- Subscribed reports
Lists all the reports to which you have already subscribed. You can see the report name, delivery date and additional subscribers. The buttons in the **Actions** column are described in the following table.
- Additional subscriptions
Lists all the reports that a manager or other person in a position of responsibility have been assigned to you. You cannot edit these reports or add other employees as subscribers. Use **Unsubscribe** in the **Actions** column to end the subscription.

To subscribe to reports:

1. Click the arrow next to the current user in the header and select **My Settings**.
The view **My Settings** is displayed.
2. Select the **Report Subscriptions** tab.
This opens the page, which is divided into three sections **Available reports**, **Subscribed reports** and **Additional subscriptions**. Use the arrow next to each section to expand the hidden list with the corresponding reports.
3. Select the report you want from **Available reports** and click **Subscribe**.
This opens the dialog box **Edit subscription settings**.
4. Click **Change** next to **Schedule**.
The dialog box **Schedule** is opened with a list of items.
5. Select how often you wish to receive the report and close the box.
6. Enter the data in all mandatory fields marked with an asterisk (*).
All unmarked fields are optional. You can also edit subscribed reports later.

 **NOTE:** If you want to subscribe to a report from an empty group, meaning a group without members, you can set the parameter value by changing **Excluded groups**. These settings are possible with the radio buttons **Active Directory® groups**, **SharePoint® groups** and **Local groups**.

7. Click **Save**.
You will find the report in **Subscribed reports**.

To obtain a report immediately

1. Click **Edit subscription settings** in the **Actions** column in the section **Subscribed reports**.
This opens the dialog box **Edit subscription settings**.
2. Click **Change** next to **Schedule**.
The dialog box **Schedule** is opened with a list of items.
3. Select an item from **Daily report subscriptions** and click **Save**.
The selected report is sent to your email address.

To end a subscription

1. Select **Unsubscribe** in the **Actions** column in the **Subscribed reports** section.
This opens a dialog box with a message.
2. Click **Yes** to unsubscribe.

To edit your report settings

1. Select **Edit subscription settings** in the **Actions** column in the section **Subscribed reports**.
This opens the dialog box **Edit subscription settings**.
2. Enter your changes or additions in the respective fields.
3. Click **Save**.

To add or remove a subscription

1. Select **Remove or add employees to this subscription** in the **Actions** column in the section **Subscribed reports**.

This opens the dialog box **Additional subscriptions**. If subscriptions have already been added, they are listed in **Current**.

2. Click on the name you want in the column **Name** in **Available** if you want to add a subscription.

- OR -

Click the filter in the column **Name** to enter a search string or to apply one of the different filter conditions.

This selected subscription is listed in **Current**.

3. Click **Save**.

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 the arrow next to the current user in the header and select **My Settings**.

The view **My Settings** is displayed.

2. Select the **My Reports** tab.

A list of reports appears.

3. Mark the report you want in the list.

A short description and other details about the selected report is displayed in the main context view.

4. Click **Show report** in the main content view.

The report is displayed as a table in the view. There are filters on the columns for you to limit the amount that is displayed.

To generate a report



NOTE: Before you export a view, you can add more columns to it, if required, using **Additional columns**.

1. Click **Export this view**.

This opens the dialog box **Export this view**. You have several options available.

2. Select either **Export as PDF**.

- OR -

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

The report is exported in the respective format.

Auditing Activity and Managing Compliance

NOTE: The term "Auditing" or "Audit" describes how an aspect of a company is assessed. An audit is normally orientated around special auditing tasks and helps quality assurance. An audit is specifically an instrument for systematic, independent and documented examination for objectively obtaining quality related activities and their evaluation based on planned requirements and targets (auditing criteria). To successfully complete and audit there must be certain features available and specific requirements must be fulfilled. (Source: sicherheitswiki.org).

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 Web Portal](#) on page 14. For more information, see:

- [Auditing - Employee Details](#) on page 92
- [Auditing - Roles and Entitlements](#) on page 96
- [Auditing - Approvals](#) on page 99
- [Auditing - Attestations](#) on page 100
- [Auditing - Rule and Policy Violations](#) on page 101

Auditing - Employee Details

For a selected employee, you can view several pages of detailed information. This information is outlined in the table below. You must select an employee before you can access the data.

To view employee details

NOTE: You will find the menu **Auditing** in the **Access Governance** main content view.

1. Select **Auditing | Employee Details**.

This opens the **Auditing - Employee Details** view with a list of employees.

2. Click **Select** next to the employee you want to view.

This opens the Auditing view for the employee with several different tabs.

Table 15: Auditing - Employee Details

Page	Details
Overview	This is the same overview shown in your profile, but for the selected employee. For more information, see Your Overview on page 83.
Requests	<p>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.</p> <p>To view a specific request in detail.</p> <ol style="list-style-type: none">1. Click Advanced search. Search settings appear on the page, which will help you to find the request you are looking for. - OR -2. Click the filter in the request list column. A dialog box appears with settings for limiting the search. - OR -3. Click the column change the to sort order from descending to ascending or the opposite. The request list resorted as required.4. Mark the request you want in the request list. This displays details of the request in the main content view. <p>For more information, see Auditing - Requests on page 98.</p>
Approvals	<p>Shows the approvals in which the selected employees participated within the selected time period. Before you can view an approval more closely, you must make a preselection. The following options are available:</p> <ul style="list-style-type: none">• Approvals (approval by approval procedure is preselected)• Exception approvals• attestation• Policy violations <p>To search for a specific approval, there is an Advanced search in the list of approvals. See the details about the Requests page on how to search. You have other settings, which you can enable or disable, in the lists on the exception approval, attestation and policy violations pages, showing the status. You can also limit the search by sorting the columns or using the filter function. For more information, see Auditing - Approvals on page 99 and Auditing - Rule and Policy Violations on page 101.</p>

Page	Details
rule violation	Shows a list of rules violations within the selected time period. You have other settings, which you can enable or disable, in the lists on the rule violations page, showing the status. You can view the status of an exception, whether it was granted or denied or still pending. You can also limit the search by sorting the columns or using the filter function. For more information, see Auditing - Rule and Policy Violations on page 101.
Risk	Shows the risk analysis for the selected employee. 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 show the risk analysis for an employee: <ol style="list-style-type: none"> 1. Click Click Auditing Employee details. 2. Select the employee you want to view 3. Click the Risk tab.
roles and entitlements	This provides you with an overview of all the employee's memberships. To view employee memberships in more detail <ol style="list-style-type: none"> 1. Sort the columns of the membership list to make it easier to find the membership you want. This resorts the columns. - OR - 2. Click the filter in the membership list column. A dialog box appears with settings for limiting the search. 3. Mark a membership to view more detailed information in main view. For more information, see Auditing - Roles and Entitlements on page 96.
Responsibilities	Provides you with an overview of the roles and entitlements functions you have been assigned, such as cost centers, business roles or system resources. Before you can view anything on this page, you must preselect an object type. To view an ownership <ol style="list-style-type: none"> 1. Select an object type in Object type. A list of objects with the selected object type appears. 2. Sort the columns to make it easier to find the ownership you want. - OR - 3. Click the filter in the ownership list column. 4. Mark a membership to view more detailed information in main view. For more information, see Auditing - Roles and Entitlements on page 96.

Page	Details
Access	<p>Shows access permissions are assigned to which governed data in the system. Before you can view access rights for a membership or resource in more detail, you must make a preselection. Memberships and Resources are available for selection:</p> <p>To view access rights</p> <ol style="list-style-type: none"> 1. Click wither Memberships or Resources. A list of corresponding objects appears. 2. Click the arrow icon next to the list item. This expands the selected item to show subitems. 3. Mark the item of choice. The access rights are displayed in one or more columns read, write and details.
History	<p>Lists all the property, membership and managerial changes and rule violations for your chosen time period. For more information, see Description of Commonly Used Tabs in Views on page 86.</p>

Changes to **Roles and Entitlements**, **Responsibilities** and **Rule Violations** effect the history.

You have the following views available to you on the **History** tab:

- Change log

The **Change log** view shows you the changes to a previously selected object in a specific time period. These changes are divided in to separate tables **Property changes**, **Memberships changes**, **Ownership changes** and **Rule violations**. The tables can be expanded or collapsed using the arrow.

In the table **Property changes**, you can see, amongst other things, the change type, the property, old and new values of the change and the change date.

The table **Memberships changes** uses data from the **Memberships** tab. You can see the change type, membership, type of membership (location, resource), user (employee that made the changes) and change date.

The table **Ownership changes** processes data from the **Ownerships** tab. This table is separated. In the top half of the table you can see the changes the selected employee manages. Bottom half contains the employees the selected employee is or was responsible for. The change type, user and change date are displayed.

The table **Rule violations** uses data from the **Rule violations** tab. The change type, rule violation, user and the change date are shown.

- State overview

The view **State overview** shows you, amongst other things, properties of the selected object and its values and length of time in this state.

- State comparison

In the **State comparison** view you can select from the **Historical state date** menu. The available data are dates on which changes were made to the selected object. If you selected a date, the data available in the tables **Properties**, **Memberships**, **Ownerships** and **Rule violations** is displayed with the current date and the selected date so that you can make a comparison. The tables can be expanded or collapsed using the arrow. If you have selected a date from the **Historical state date** menu, you can use the arrow buttons below it to select an earlier or later date to compare with the current date.

To view changes to specific employees

1. Click **Auditing | Employee Details**
2. Click **Select** the employee you want from the list of employees shown.
3. Mark the membership on **Roles and entitlements** tab, if required.

This displays details of the membership in the main content view.

Auditing - Roles and Entitlements

You can use this view to get historical information about an employee's roles, entitlements and other business ownerships:

- Related Applications
- business roles
- Cost Centers
- Data objects under governance
- Departments
- Employees
- ManagerApplication Roles
- Locations
- Resources
- System entitlements
- System Roles

Once you locate the item you are looking for, you can drill in and examine the details. For more information, see [Managing "My Responsibilities"](#) on page 56. The available details depend on the item you are exploring and want to check. Many contain the following overviews:

- Overview
- Memberships
- Master Data
- entitlement
- Risk
- Compliance
- attestation
- Usage
- History

For more information on the information on these tabs, see [Description of Commonly Used Tabs in Views](#) on page 86

Changes to **Memberships**, **Master data** and **Entitlements** effect the history.



NOTE: You see these overviews when you select **Organizations, Departments, Locations** or **Cost centers** objects.

You have the following views available to you on the **History** tab:

- **Change log**

The **Change log** view shows you the changes to a previously selected object in a specific time period. These changes are divided in to separate tables **Property changes**, **Memberships changes** and **Entitlement changes**.

The table **Property changes** uses data from the **Master data** tab. You can see, amongst other things, the change type, the property, old and new values of the change and the change date.

The table **Memberships changes** uses data from the **Memberships** tab. You can see the change type, membership, type of membership (primary, secondary) and change date.

The table **Entitlement changes** processes data from the **Entitlement changes** tab. The change type, entitlement, type of entitlement are displayed.

- **State overview**

The view **State overview** shows you in the table **Historical state date**, amongst other things, properties of the selected object and its values and length of time in this state.

- **State comparison**

In the **State comparison** view you can select from the **Historical state date** menu. The available data are dates on which changes were made to the selected object. If you selected a date, the data available in the tables **Properties**, **Memberships**, **Entitlements** is displayed with the current date and the selected date so that you can make a comparison. If you have selected a date from the **Historical state date** menu, you can use the arrow buttons below it to select an earlier or later date to compare with the current date.

To view historical details about a specific role or entitlement

1. Click **Auditing | Roles and Entitlements**.

2. Select the category or a specific role or entitlement.

This opens a dialog box for the selected object.

3. Click **Assign** next to the **Select employee**.

4. Click the filter in the result list column.

A dialog box appears with settings for limiting the search.

- OR -

5. Click the column change the to sort order from descending to ascending or the opposite.

The request list resorted as required.

6. Mark the request you want in the request list.

This displays details of the request in the main content view.

To view all the roles or entitlements for a specific employee


1. Select **Auditing | Roles and Entitlements**.

2. Select the category or a specific role or entitlement.


This opens a dialog box for the selected object.

3. Click **Assign** next to the **Select employee**
This opens the dialog box **Select employee**.
4. Select the employee you want to view.
Any roles and entitlements for the selected employee appear, grouped by category.
5. Mark the item of choice in the results list.
This displays details of the selected item in the main content view.

To change the access permissions for an Active Directory® resource

 **NOTE:** This function is only available when the module Data Governance Module is installed.

1. Click **Auditing | Roles and Entitlements**.
This opens the **Auditing | Roles and Entitlements** view.
2. Click the Active Directory® element.
This opens the **Overview** with a list of Active Directory® resources.
3. Click **Assign** next to the **Select employee**
This opens the dialog box **Select employee**.
4. Select the employee you want to view.
5. Click the Active Directory® resource you want, and then select **Access**.
6. Click the plus sign next to the group to extend the list and view parent groups.

 **NOTE:** If more parent groups are shown with a plus sign, click on it until either a folder or a file is shown. This means you can also view access permissions for parent groups.

A check marks are displayed in the columns **Read**, **Write** of the select system entitlement and a button in the **Details** column. Read/write access is given to the file or folder depending on the columns in which these check marks are shown.

7. Select **Details** next to the file or folder.
This opens the dialog box **Access Control List** showing the assigned permissions.

Auditing - Requests


This overview lists all requests that have been created with the selected time period. You can select an employee to only show this employee's requests. Furthermore, you can use the filter and sort functions or the advanced search on the columns of the list to limit the requests or display more columns. For more information on making and processing requests, see [Making and Managing Requests](#) on page 25. For each request, you can see a variety of information in the main 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. Click **Auditing | Requests**.
2. Click **Assign** next to the **Select employee**
This opens the dialog box **Employee**.
3. Select the employee you want from the list of employees shown.
- OR -
4. Click **Advanced Search** to enter more search parameters.
A list of requests appears in the bottom pane.
5. Mark the request you want in the request list.
This displays details of the request in the main content view.


 **NOTE:** The **Workflow** tab shows you all changes in chronological order in the form of a workflow graphic. The **Cart** button shows you the request number and requester in a dialog box.

Auditing - Approvals


You can use the **Auditing - Approvals** page to see the requests in which a particular employee was involved. This view is the same as the **Auditing - Requests** view with a customized filter. For more information, see [Auditing - Requests](#) on page 98. You can narrow down the requests by a date range, or use advanced search to provide more filters. For more information, see [Auditing - Requests](#) on page 98.

To view all historical requests for a specific approver

1. Click **Auditing | Approvals**.
2. Click the link **assign** next to **Select approver**.
This opens the dialog box **Employee**.
3. Select the employee you want from the list of employees shown.
- OR -
4. Click **Advanced Search** to enter more search parameters.
A list of all the requests approved by the selected employee, or open requests that could be approved by the selected employee appears in the bottom pane.
5. Mark the request you want in the request list.
This displays details of the request in the main content view.

 **NOTE:** The **Workflow** tab shows you all changes in chronological order in the form of a workflow graphic. The **Cart** button shows you the request number and requester in a dialog box.

Auditing - Attestations


 **NOTE:** This function is only available if the Attestation Module module is installed.

Use the **Auditing - Attestations** view to see attestation cases within a specified time period. The content and type of view vary in presentation depending on the respective company. You can may be able to view:

- Attestation policy
- Attestation case
- Creation date
- Due date
- Approval status
 - Pending
 - Approved
 - Denied

To view historical attestation data


1. Click **Auditing | Attestations**.
2. Click the link **assign** next to **Approver**.
This opens the dialog box **Employee**.
3. Select the employee you want from the list of employees shown.
The selected employee is displayed in the view, **Auditing - Attestations** next to **Select approver**.
4. Enable or disable one or more of the check boxes next to **Attestation state**.

 **NOTE:** You can use the filter and sort functions to limit the results on the columns or display more columns.

A list of all the matching attestation cases, grouped by attestation policy appears in the bottom pane.

5. Mark the attestation policy to view the desired attestation case.
You can view more information in the main content view under the tabs **Information**, **Workflow**, **Attestation policy** and **History**.


To notify an approver about pending attestation cases

 **NOTE:** You can only contact approvers for attestation cases which have the status **Pending**.

1. Select the attestation case as in **To view historical attestation data**.
2. Click **View approvers for pending cases** at the bottom of the **Auditing - Attestations** view.
This opens the dialog box **Send a reminder mail** with a list of approvers, who must still approve pending attestation cases.
3. Click **Send a mail** next to the employee to notify.
The email program linked to the Web Designer is displayed and an email template with the approver's email address is opened.

4. Write and send the email to the approver.
The email program is closed.

Auditing - Rule and Policy Violations

 **NOTE:** This function is available if the Company Policies Module or Compliance Rules Module module is installed.

You can view all employees who have violated rule under the menu item **Rule Violations**. 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. The following information is provided in a violations view:


- The violated employee or object.
- The rule or policy being violated.
- The state of the exception approval:
 - exception approved
 - exception denied
 - pending

Click on the state to see the reason for the decision.

- The approver if approved or denied.
- Approval date.

To view historical rule or policy violation data

1. Click **Auditing | Rule Violations** to view rule violations.
- OR -
2. Click **Auditing | Rule Violations** to view policy violations.
3. Click the link **assign** next to **Select approver**.
This opens the dialog box **Employee**.
4. Select the employee you want from the list of employees shown.
The selected employee is displayed in the view, **Auditing - Rule Violations** or **Auditing - Policy Violations**, next to **Select approver**.
5. Enable or disable one or more of the check boxes next to **State**.


 **NOTE:** You can use the filter and sort functions to limit the results on the columns or display more columns.

A list of all the matching rule or policy violations appears in the bottom part of the content view.

6. Mark the violation to view it in more detail in the main content view.

You can view more information in the main content view under the tabs **Rule violation** and **Rule** and also **Policy violation**, **Object** and **Policy**.

Working with Compliance

 **NOTE:** This function is only available when the module Compliance Rules Module or Governance Base 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).

- 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, for example, 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 Identity Manager solution to reduce the risks posed by the violation. Reports and dashboards give you further insights into your state of compliance. For information on the Compliance dashboard, see [What Statistics are Available?](#) on page 80.

Compliance activities can include:

- [Assigning Resource Owners](#)
- [Modifying Risk Calculators](#)
- [Performing Attestations](#)
- [Viewing Compliance Frameworks](#)
- [Managing Rule and Policy Violations](#)

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 table outlines the compliance based information you may see, and the role you need in order to see it.

Table 16: 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 enabled in the Manager.	Attestation administrator, policy administrator, compliance rule administrator


View	Description	roles
Attestation policies	Lists attestation policies, and allows editing of existing and creation of new policies.	Compliance officer, attestation administrator
Policy violations	Provides reports on objects which violate policies.	Framework administrator, policy administrator, policy approver
Compliance Frameworks	Provided details about the compliance frameworks in your environment.	Compliance framework administrator
rule violation	Provides reports on employees who violate policies.	Framework administrator, rule administrator 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 compliance rules related to SAP functions. SAP rights calculation must be enabled. SAP permissions calculation must be enabled by an administrator.	Compliance framework administrator
function analysis	Identifies employees who are improperly assigned to critical SAP functions. SAP functions calculation must be enabled by an administrator.	rule supervisor

Assigning Resource Owners

Data Governance provides a systematic approach to managing data access, preserving data integrity, and providing you with the tools and workflows to manage your own data resources, without relying on IT administrators. By evaluating resource access, you can identify resources that do not have ownership, assign owners, and assess the overall ownership of your governed data.

 **NOTE:** You will find the menu **Governed Data** in the **Access Governance** main content view.

It is important that governed resources have owners. Owners can use the Web Portal to manage access to the resource, without the specialized IT knowledge that was previously needed. Owners are better positioned than IT staff to understand what employees require specific levels of access to their resources. You can manipulate the views to maximize their value, and export the information to a report. For more information, see [Tips for using Web Portal](#) on page 14. Resources without owners may violate company policies. For more information, see [Managing Rule and Policy Violations](#) on page 116.

 **NOTE:** Once a resource has been assigned an owner, it appears on the **My Responsibilities | File System** or **SharePoint®** for the selected employee. They can then manage the resource. For more information, see [Working with File System and SharePoint® Resources](#) on page 62.

You can view:

- Overview of various resources

There is a tab for the various resources. Depending on which resource types exist, you can view, for example, the data for resources assigned to owners in percent.

- Resources without Ownership

Lists all resources that are governed but have no owners. The Manager can recommend a perceived owner for some resources. This recommendation is calculated based on the activity on the resource. For example, an employee who created and has made changes to a Word document is more likely to be its owner than one who has read the document once.



NOTE: Recommendations are only available for resources for which activity tracking is enabled by an administrator.

To view an overview all existing resources

1. Click **Governed Data | View Resources**.

The **View Resources** view has a number of different tabs.

2. Select a tab to view a specific resource type.

A list of resources of the selected type appear. Depending on your environment, you may have hNTFSave or oSharePoint resources. You can click on each resource in the list.

3. Click the resource you want.

A new view with detailed information about the resource is distributed over several tabs.

To assign an owner to a resource

1. Select **Governed Data | View Resources**.

The **View Resources** view has a number of different tabs.

2. Select the **Resources without ownership** tab.

A list of resources appear. Depending on your environment, you may have hNTFSave or oSharePoint resources. Resources assigned an owner have an **Assign** button.

3. Enable the check box in the **Governed data name** column.

You can select multiple resources if you are assigning the same owner.

4. Click **Assign owner**.

This opens the dialog box **Assign owner**.

5. Click **Assign** next to the **Select employee**

The **Owner** view is displayed.

6. Select an employee from the list of owners shown.

The selected owner is displayed next to **Select employee** in the dialog box **Assign employee**.

7. Click **Assign owner**.

To modify the master data of a resource (this needs verification)

1. Select **Governed Data | View Resources**.

The **View Resources** view has a number of different tabs.

2. Select a tab to view a specific resource type.

A list of resources of the selected type appear. Depending on your environment, you may have hSharePoint or NTFS resources. You can click on each resource in the list.

3. Click the resource you want.

A new view with detailed information about the resource is distributed over several tabs.

4. Select the tab **Master data**.
5. Select the data you want to edit.
6. Click **Save** to save the changes.

- OR -


Click **Delete** if you want to remove the resources.

- OR -

Click **Discard changes** if you do not want to accept the changes.

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 Manager, risk data is gathered from a variety of sources, and then calculations are performed to produce risk indexes. Every item within the Manager can be assigned a risk value. If you own resources, you may be 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 69.

 **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:

- **Average**
Averages the risk indexes of the objects affected by the function.
- **Maximum**
Uses the maximum value of the risk indexes of all objects affected
- **Increment**
Increments the risk by a constant value
- **Decrement**
Decrements the risk by a constant value

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 **High Risk Overview**. For more information, see [What Statistics are Available?](#) on page 80.

To modify a risk index function


1. Click **Administration | Risk Assessment**.
2. Select the risk index function and click **Edit**.
This opens a dialog box.
3. Select the type in **Calculation type** menu.

4. Click in **Weighting** and change the risk index.
5. Click **Save**.


To disable or enable a risk index function

1. Click **Administration | Risk Assessment**.
2. Select the risk index function and click **Edit**.
3. Check or uncheck the **Disabled** box as required.
4. Click **Save**.

Performing Attestations

 **NOTE:** This function is only available when the module Governance Base Module or Attestation Module is installed.

Managers or others responsible for compliance can use Manager attestation policies to certify access permissions, authorizations, requests and exception approvals. Attestations start with attestation policies. You use these policies to specify which objects are designated for attestation, who performs the attestation, when and how frequently the attestations should be carried out. 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 80.

 **NOTE:** The main menu **Governance Administration** must be selected in order to select the menu **Administration | Attestation Policies**. For more information, see [Navigating around the Web Portal](#) on page 9.

The following activities are involved in the attestation process:

- [Working with Attestation Policies](#)
- [Select Object Link Types](#)
- [Approving and Denying Attestations](#)
- [Viewing Completed Attestations](#)

Working with Attestation Policies

If you are responsible for attestation policies, you can work with the **Attestation Policies** menu.

Attestation policies generate attestation cases to schedule. Each attestation case must be granted or denied approval by an authorized employee. You can also configure the system to close obsolete attestation cases. You can set up and edit conditions when editing attestation policies. This function makes it possible for you to view all objects adhering to a certain condition. For more information, refer to [Approving and Denying Attestations](#) on page 112.

Not all fields of an existing policy can be edited. This depends on your access permissions. All attestation policies with the following information on the tabs **Attestation Policy Settings** and **Attestation Policy Runs** are displayed when you select the menu item **Attestation Policies**.

Table 17: Attestation policy - "Attestation Policy Settings"

Column	Description
Attestation policy	Name of the attestation policy.
Attestation procedure	Name of the attestation procedure.
compliance framework	Frameworks are used for classifying company policies and compliance rules 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:** If you want to view all policies, you must check the option **Show disabled policies** at the bottom of the table.

Table 18: 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 19: Description of the Main Content

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
Role approver	On the Approver tab, you will find information about pending and closed approvals and the approvers involved for the selected attestation run. 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.

To send a reminder to an approver


1. Click **Administration | Attestation policies**.

 **NOTE:** Next to **Min. category**, you can change between **Good**, **Mediocre** and **Bad** to limit the attestation policies shown.

2. Select for the attestation policy.

More details about the selected attestation are displayed in the main content view.

3. Enable the check box next to the approver on the **Approvers** tab.

 **NOTE:** You can multi-select approvers or you can select all approvers by setting the last check box in the list.


4. Click **Send reminder**.


To edit an attestation policy

1. Click **Administration | Attestation policies**.

2. Click the tab **Manage attestation policies**.

3. Select an attestation policy in the attestation policy overview and click **Edit attestation policy** in **Actions**.

 **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**. If you want to make changes to a default attestation policy, create a copy and edit the copy.

 **NOTE:** If the check box **Close obsolete tasks automatically** is set, you cannot hide processed attestation cases which are beyond the deadline.

4. Edit the data you want to change.

You can also add new conditions, change or delete existing ones. Your permissions determined which data you may edit.

5. Click **Save**.

To add or delete a policy condition

1. Click **Administration | Attestation policies**.

2. Click the tab **Manage attestation policies**.

3. Edit an attestation policy.

4. Click **Delete Condition** in the **Object selection** part of the **Edit attestation policy** view to delete an existing condition.

- OR -

Click **Edit condition** in the **Object selection** part of the **Edit attestation policy** view to create a new condition.

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

5. Select the option you want in **Condition type**.



NOTE: The options available in **Condition type** depend on which attestation procedure is set for the attestation policy to be edited.

6. Enter the rest of the data for the chosen option.

Which other data is required depends on the option selected.

7. Click **Ok**, once you have selected a condition type and entered the corresponding data.

8. Click **Ok**, once you have specified a threshold.

To add a condition, which includes objects whose names contain a specific string

1. Click **Administration | Attestation policies**.
2. Click the tab **Manage attestation policies**.
3. Select an attestation policy or add a new one.
4. Click **Edit condition** or **Add another condition** in the **Object selection** part of the **Edit attestation policy** view in the **Actions** column.

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

5. Select the option **...with matching name in condition type**.
6. Enter part of the name to filter the object by in **Name**.
7. Click **OK**.

To edit a policy condition

1. Click **Attestation | Attestation policies**.
2. Click the tab **Manage attestation policies**.
3. Edit an attestation policy.
4. Select the condition you want to modify in view with the object selection and click **Edit condition** in **Actions**.
5. Select the setting you want.
6. Click **OK** to confirm.

To display all objects for attestation after applying a filter for valid conditions

1. Click **Attestation | Attestation policies**.
2. Click the tab **Manage attestation policies**.
3. Edit an attestation policy.
4. Click the linked number of the condition you want in the **Object** column in the section **Object selection**.

- OR -

Click The linked number below the list of all conditions.

All objects which meet the condition/s are displayed in a dialog box.

To update the object selection list

1. Click **Administration | Attestation policies**.
2. Click the tab **Manage attestation policies**.
3. Edit an attestation policy.
4. Click **Reload matching objects** below the list of all conditions.

This reloads the object selection. New conditions, which may also be added to the Manager, are also shown. For more information, see the Dell One Identity Manager Attestation Administration Guide.

To create a new attestation policy

1. Click **Administration | Attestation policies**.
2. Click the tab **Manage attestation policies**.
3. Click **Create new attestation policy**.
4. Enter a unique name for the attestation policy.
5. Click the link **Assign** next to **Attestation procedure** and select an attestation procedure.

The search can be simplified if you search within an attestation procedure.



NOTE: Your choice of attestation procedure in **Attestation procedure** is critical for create a new attestation policy. 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.

6. Click the link **Assign** next to **Approval policy** and select the approval policy from list.
7. Click the link **Assign** next to **Calculation schedule** and select the deadline from list.
8. Enter the number of days within which to approve the attestation case in **Time required [days]**.
9. Enable **Close obsolete tasks automatically** to close pending attestation cases from previous attestation runs during an attestation run.
10. Click the link **Assign** next to **Compliance Framework** and select the corresponding rule from the list.
You can select multiple frameworks, if required.
11. Enter additional information about the attestation policy in in **Description**.
12. Enter more conditions as necessary.
13. Change the condition's link type, if required.
14. Click **Create**.

To create a new attestation policy based on an existing policy

1. Select **Governance Administration | Attestation policies**.
2. Click the tab **Manage attestation policies**.
3. Select the basis policy and click **Copy attestation policy**.

4. Click **Yes** in the dialog box.
5. Edit the policy as desired.
6. Enable filter criteria, if required.
7. Click **Save**.

Select Object Link Types

Before you save data or change 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:


- All conditions must be met. New attestation cases are added for all objects fulfilling each of the 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 met. 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.

Example: 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

 **NOTE:** You can modify this setting when you add or edit a new attestation policy.

1. Click **Administration | Attestation policies**.
2. Select the tab **Manage attestation policies**.
3. Click **Edit attestation policy** in the column **Actions** of the attestation policy you want edit.
This opens the page **Create new attestation policy** or **Edit attestation policy** respectively.
4. Click **Change** next to **Attestation procedure**.
This opens the dialog box **Attestation procedure**.
5. Click the arrow in the list to make a further selection from the link type.
6. Mark the desired link type.
This accepts the changes and the dialog window is closed. You are returned to the **Edit attestation policy** or **Create new attestation policy** view.
7. Click **Create** or **Save** respectively.

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 needs to be attested to, and by whom. Attestation policies are run on a schedule, and generate attestation cases. These appear on the **My Actions** menu. The amount of time you are given 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 9.


As an attestor, you must be able to verify your attestation. This may require running reports or manually verifying the objects to which you are attesting. If you are not ready to make a decision, you may be able to:

- Generate a report that provides detailed information about the object to which you are attesting
- Request more information, add attestors, or delegate the attestation. For more information, see [Handling Requests when You Need More Information](#) on page 47.

For more information about how Attestations can be audited, see [Auditing - Attestations](#) on page 100.

To generate a report to provide you with information for the attestation case

1. Select **My Actions | Pending Attestations**.
A list of policies with attestation cases appears.
2. Select the policy you want.
This displays a list of attestation cases.
3. Mark the desired attestation case in the list.
This displays details of the case in the main content view.

 **NOTE:** Not all attestation cases have reports available.

4. Click **Report** in the main content view.
This generates a PDF.

To approve or deny an attestation case

1. Select **My Actions | Pending Attestations**.
A list of policies with attestation cases appears.
2. Select the policy you want.
This displays a list of attestation cases.
3. Click either the check box to **Grant** or **Deny** approval in the **Decision** column.
4. Enter a reason to support your approval decision in the text box.
- OR -
5. Click **Assign** next to **Standard reason**.
The dialog box **Standard reasons** is opened with a list of reasons.
6. Select a reason from the list.

This closes the the dialog box and the selected reason is displayed next to **Standard reason**.

i | **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 standard reasons, see the Dell One Identity Manager IT Shop Administration Guide.

7. Click **Save approvals**.

i | **NOTE:** If you want to grant or deny approval to the entire list of visible attestation cases, you can set the options **Approve all** or **Deny all** before you click **Save approvals**.

To view an attestation object

1. Select **My Actions | Pending Attestations**.
A list of policies with attestation cases appears.
2. Select the policy you want.
This displays a list of attestation cases.
3. Select the desired attestation case.
This displays details of the case in the main content view.
4. Click the link **Actions** and select the item **Go to attested object**.
This opens a view for the selected object.

To view attestation for a specific object type

1. Select **My Actions | Pending Attestations**.
A list of policies with attestation cases appears.
2. Select the tab **Object types**.
This displays a list with several object types to choose from.

i | **NOTE:** How you proceed, depends on the object type you select.

3. Select the table for the object type you want.
 - a. Proceed as follows, if you have selected object types **Department**, **location** or **Organization** in **Table**.
A list appears in the view for your selected object types.
 - b. Select the object type you want, for example, department.
This display a view with the pending attestations for the selected object types. The tabs **All attestation cases**, **Entitlements**, **Memberships** and **Member entitlements** help you to group the view further.
- OR -
- a. Proceed as follows, if you have selected the object type **Employees** or **System entitlements** in **Table**.
A list appears in the view for your selected object types.
 - b. Select the object type for which you want to view the attestation, for example, employee.

The tab **Group memberships** and **All attestation cases** are available in the **Pending attestations** view.

4. Select the tab you want to view.

This displays a list of attestation cases for the selected tab.

5. Mark the attestation you want to view in detail.

In the mail content view you see several tab containing detailed information about attestation.

To send a reminder to an approver

1. Select **My Actions | Pending Attestations**.

A list of policies with attestation cases appears.

2. Select the policy you want.

This displays a list of attestation cases.

3. Select the attestation case.

This displays details of the case in the main content view.

4. Click the link **Actions** and select **Send a reminder** from the context menu.

This opens the dialog box **Send a reminder**, with a list of employees who may approve the attestation case.

5. Click **Send a mail** next to the employee to notify.

The email program linked to the Web Designer is displayed and an email template with the approver's email address is opened.

6. Write and send the email to the approver.

The email program is closed.

To view employees with approval authorization for an attestation case

1. Select **My Actions | Pending Attestations**.

A list of policies with attestation cases appears.

2. Select the policy you want.

This displays a list of attestation cases.

3. Select the attestation case.

This displays details of the case in the main content view.

4. 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. Select **My Actions | Pending Attestations**.

A list of policies with attestation cases appears.

2. Select the policy you want.

This displays a list of attestation cases.

3. Select the attestation case.


This displays details of the case in the main content view.

4. Select the **History** tab.

This displays a list of the attestation cases that have already taken place for the selected object. You can call up more information about each attestation case with the Information button.

Editing Attestation with the Chief Approval Team

If there are attestations 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 information, see the Dell One Identity Manager IT Shop 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

- Click **My Actions | Attestation Escalation Approvals**.

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 112.


 **IMPORTANT:** The four-eye rule can be broken like this because chief approval team members can make approval decisions for 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 84 and [Auditing - Attestations](#) on page 100.

 **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 9.


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. Click **Administration | Attestation policies**.

The **Attestation policies** view is displayed including your own attestation policies, if this applies.


 **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 in the view.

2. Mark the attestation policy in the list that you want to view.


More information about the policy is displayed in the main content view. For more information about details in the main context view, see the table **Description of the Main Content** in [Working with Attestation Policies](#) on page 106.

 | **NOTE:** If you have no other permissions, you can only view your attestation policies.

Viewing Compliance Frameworks

 | **NOTE:** This function is only available when the module Governance Base 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. For example, if you are required to comply with a particular framework, it is helpful to know which rule, policies and attestation policies are associated 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 9.

To view a compliance framework

1. Select **Compliance | Compliance Frameworks**.
A list of frameworks with their managers appear.
2. Select a framework.
A hyperview of the framework appears, with a shape for the associated rules, policies and attestation policies. For more information, see [Tips for using Web Portal](#) on page 14.

Managing Rule and Policy Violations

Not adhering to rules and policies 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 appear on your **My Actions** menu. You can see:


- Employees or objects that have violated the rule or policy.
- The rule or policy that each violated.
- The status of the exception approval. There are 3 possibilities:
 - Pending


- Exception granted
- Exception denied
- For policies, the date the violation was detected.
- Employees who have denied or granted exception approval.
- The approval date for each approver.

If you are an auditor or manager, you can view historical information about exception decisions. For more information, see [Auditing - Rule and Policy Violations](#) on page 101.

To grant or deny exception approvals

1. Select **My Actions | Pending Rule Violations** for rule exceptions.
The view **Pending Rule Violations** is displayed.
- OR -
2. Select **My Actions | Pending Policy Violations** for policy exceptions.
The view **Pending Rule Violations** is displayed.
3. Enable one of the following check boxes to limit the display of rule or policy violations:
 - Exception granted
 - Exception denied
 - Pending
 Only the rule or policy violations of the selected type are displayed.
4. Mark the rule or policy violation you want in the list.
This displays details of the violation in the main content view and you can carry out various actions. How you continue, depends on the view you find yourself in.
5. Click either **Granted** or **Denied** in the **Decision** column.
Your selected is highlighted.
6. To edit a rule or policy violation
 - a. Click **Assign** next to **Mitigating control** in the main context view on the **rule violation** or **Policy violation** tab respectively.
This opens the **Assign** view with the sections **Available** and **Assigned**. You are offered a list of mitigating controls under **Available**.
 - b. Select an entry in **Available** and click **OK**.
Assigns the selected mitigating control to the case.
 **NOTE:** If you want to change a mitigating control, click **Change** next to the **Item**.
 - c. Click **Next** in the main context view.
This displays the **Approval exceptions** view.
 - d. Enter a reason for your decision in **Reason for approvals** or **Reason for denials**.
- OR -
Select a predefined and saved reason in **Standard 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 standard reasons, see the Dell One Identity Manager IT Shop Administration Guide.

 **NOTE:** If you are editing several rule or policy violations, you have the option to enter a reason for each one individually by clicking the link **Enter reason** in the **Reason** column.

- e. Click **Save approval** when you have finished editing.

Your approval decision is saved and the policy violation's status changes accordingly.

To view the history of your exception decisions

1. Select **My Actions | Rule Violation History** for rule exceptions.

- OR -


Select **My Actions | Policy Violations** for policy exceptions.

2. Enable on of the check boxes **Exception granted**, **Exception denied** to limit the number of historical rule and policy violations displayed.

Only historical rule or policy violations of the selected type are displayed.

3. Select the rule or policy violation in the list.

This displays details of the violation in the main 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 determining policy violations within their 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 Manager solution and which reduce the risk of violation. For more information, see [Working with Compliance](#) on page 102.

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 3 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

i | **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 radio buttons in your rule violation view are visible to you:

- By framework
- By department
- By rule
- By application role
- All compliance rules

i | **NOTE:** If you only have an application The radio button corresponding to the application in this case are preset and must not be enabled by you.

To view rule violations

1. Select **Compliance | Rule violations**.
2. Set the radio buttons shown, to present the view more clearly.
3. Select a framework.

- OR -

Select a rule.

Depending on your role assignment, you can generate a report using **Report about rules** or **Report about policies**.

Depending on which application is assigned to you, the following radio buttons in your rule violation view are visible to you:

- Framework administrator
- All Policies

To view rule violations

1. Select **Compliance | Rule violations**.
2. Set the radio buttons shown, to present the view more clearly.
3. Select a framework.

- OR -

Select a policy.

Depending on your role assignment, you can generate a report using **Report about rules** or **Report about policies**.

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.
- **Critical 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 action. If a rule of high significance is violated on an SAP function of significance, immediate action should be taken.

To analyze compliance rule violations for rules that contain SAP functions

1. Select **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. To analyze by role, Click **By role**, and then expand each role and profile to view the violation details.
4. Click **Back** to return to the list of employees.
5. To analyze by ability, Click **By ability** expand the SAP functions and transactions to see details.

To identify employees who violate compliance rules with critical SAP functions

1. Select **Compliance | Critical Function Analysis**.
A list of employees with critical SAP functions appears.
2. To view the details of the SAP functions and compliance rules involved in the violation, locate an employee and Click **Select**.

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell Software

Technical Support:

[Online Support](#)

Product Questions and Sales:

(800) 306 - 9329

Email:

info@software.dell.com

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 <http://software.dell.com/support/>.

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 portal provides direct access to product support engineers through an online Service Request system.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to [Trial Downloads](#).
- View how-to videos
- Engage in community discussions
- Chat with a support engineer

A

Approval History

view 51

attestation

Approving and Denying Attestations 112

execute 106

managing attestation policies 106

Viewing Completed Attestations 115

Auditing

approvals 99

attestation 100

employee details 92

requests 98

roles and entitlements 96

rule and policy violation 101

B

business roles

edit master data 69

manage 56

C

Compliance

compliance admin 102

compliance framework

Viewing Compliance Frameworks 116

contact data

rework 8

D

delegation history

call 55

E

employees

add 70

edit 70

F

file system

manage 62

function analysis 120

H

home page 10

M

Menu Bar 10

My Business Ownerships

manage 56

O

organization structure

manage 56

Other applications

ace 74

other services

edit master data 69

manage 65

P

pending question

answer 50

R

report

generate 89

- subscribe 89
- view 91
- request templates
 - create 34
 - edit 34
- requests
 - act 26
 - about a product group 28
 - about a reference user 30
 - for other recipient 31
 - from template 29
 - edit pending request 43, 47
 - extend 33
 - manage 25
 - more edit options for pending requests 47
 - process monitoring 41
 - repeat 33
 - request email notification 52
 - request group 36
 - request resource 36
 - revoke 42
 - shopping cart aid 37
 - special request 35

Resources

- Assigning Resource Owners 103

Risk Assessment

- Modifying Risk Calculators 105

roles

- delegate 53

Rule analysis 120

rule and policy violation

- edit pending violations 116

- manage 116

- view reports about rule and policy violation 118

S

SharePoint® resources

- manage 62

System entitlements

- manage 58

System Roles

- edit master data 69

- manage 56

W

Web Portal

- log in 7

- log out 7

- navigate 9

- search 75

- tips for use 14