



One Identity Manager

Web Portal User Guide

**Copyright 2021 One Identity LLC.**

**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 One Identity LLC.

The information in this document is provided in connection with One Identity 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 One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY 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 ONE IDENTITY 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 ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity 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. One Identity 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:

One Identity LLC.  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

**Patents**

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

**Trademarks**

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at [www.OneIdentity.com/legal](http://www.OneIdentity.com/legal). All other trademarks are the property of their respective owners.

**Legend**

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

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

# Contents

<b>General tips and getting started .....</b>	<b>9</b>
Logging in and out .....	10
Logging in .....	10
Logging in to the Password Reset Portal .....	11
Logging off .....	12
Navigation and use .....	12
Simple navigation .....	13
Search .....	14
Context searching .....	15
Help .....	15
Using the help .....	15
Filtering .....	16
Displaying the address book .....	16
Managing password questions .....	16
Creating password questions .....	17
Editing password questions .....	17
Deleting password questions .....	18
Changing passwords .....	18
Switching languages .....	19
Enabling/disabling email notifications .....	19
Report subscriptions management .....	20
Subscribing to reports .....	20
Editing report subscriptions .....	21
Sending reports from report subscriptions .....	22
Unsubscribing reports .....	22
The user interface layout .....	23
Home .....	23
Header .....	23
Menu bar .....	24
<b>Requests .....</b>	<b>25</b>
Requesting products .....	26

Adding products to the shopping cart .....	26
Managing products in the shopping cart .....	27
Displaying the shopping cart .....	28
Removing products from the shopping cart .....	29
Setting the validity period of products in your shopping cart .....	30
Specifying the priority of products in your shopping cart .....	30
Giving reasons for requests .....	31
Checking the shopping cart .....	31
Requesting products in the shopping cart for multiple identities .....	32
Deleting shopping carts .....	33
Submitting requests .....	33
Displaying and requesting other identity's products .....	34
Requesting products through reference users .....	34
Requesting products through peer groups .....	35
Requesting for other identities or subidentities .....	36
Requests for Active Directory groups .....	36
Requesting new Active Directory groups .....	37
Requesting changes to Active Directory groups .....	38
Requesting deletion of Active Directory groups .....	39
Saved for Later list .....	39
Saving products for later .....	39
Displaying Saved for Later list .....	40
Requesting products on the Saved for Later list .....	40
Removing products from the Saved for Later list .....	41
Deleting the Saved for Later list .....	42
Pending requests .....	42
Displaying pending requests .....	43
Approving and denying requests .....	43
Approving pending requests from newly created Active Directory groups .....	44
Appointing other approvers for pending requests .....	45
Rerouting approvals of pending requests .....	46
Appointing additional approvers to pending requests .....	46
Delegating approvals of pending requests to other identities .....	48
Rejecting request approval .....	49
Displaying request history .....	50

Canceling requests .....	51
Renewing products with limit validity periods .....	51
Unsubscribing products .....	53
Displaying approvals .....	54
Undoing approvals .....	54
<b>Attestation .....</b>	<b>56</b>
Sending attestation reminders .....	56
Sending reminders about attestation runs .....	57
Pending attestations .....	57
Displaying pending attestation cases .....	58
Granting or denying attestation cases .....	58
Appointing other approvers for pending attestation cases .....	59
Rerouting approvals of pending attestation cases .....	60
Appointing additional approvers to pending attestation cases .....	61
Delegating approvals of pending attestation cases to other identities .....	63
Rejecting approval of attestation cases .....	65
Displaying attestation history .....	66
Attestation – Administration .....	66
Attestation policies .....	67
Displaying attestation policies .....	67
Displaying attestation policy reports .....	68
Setting up attestation policies .....	68
Editing attestation policies .....	71
Copying attestation policies .....	73
Deleting attestation policies .....	76
Starting attestation .....	76
Attestation runs .....	77
Displaying attestation policy runs .....	77
Displaying attestation cases of application runs .....	78
Displaying attestation run reports .....	79
Extending attestation runs .....	79
Attestation by peer group analysis .....	79
<b>Responsibilities .....</b>	<b>81</b>
My responsibilities .....	81

My identities .....	81
Displaying my identities .....	82
Deactivating my identities .....	82
My identities' attestations .....	83
Delegating tasks .....	85
Displaying delegations .....	85
Creating delegations .....	85
Canceling delegations .....	86
Deleting delegations .....	87
Ownerships .....	87
Assigning product owners to system entitlements .....	88
<b>Setting up and configuring request functions .....</b>	<b>89</b>
Managing shops .....	89
Displaying shops .....	90
Creating shops .....	90
Editing shops .....	91
Editing shop details .....	92
Deleting shops .....	92
Managing shop shelves .....	93
Displaying shop shelves .....	93
Creating shelves for shops .....	93
Editing shop shelves .....	94
Deleting shelves from shops .....	96
Managing access to requestable system entitlements in shops .....	96
Displaying shop members .....	96
Adding members to shops .....	97
Removing members from shops .....	97
Managing requestable products in shops .....	97
Displaying requestable products .....	98
Adding products to shelves .....	98
Removing products from shelves .....	99
<b>Appendix: Attestation conditions and approval policies from attestation procedures .....</b>	<b>100</b>
Attesting primary departments .....	100
Attesting primary business roles .....	101

Attesting primary cost centers .....	102
Attesting primary locations .....	102
Attesting secondary departments .....	103
Attesting secondary cost centers .....	104
Attesting secondary locations .....	104
Attesting PAM asset groups .....	105
Attesting PAM asset accounts .....	105
Attesting PAM assets .....	106
Attesting PAM user groups .....	106
Attesting PAM user accounts .....	107
Attesting PAM account groups .....	108
Attesting PAM directory accounts .....	108
Attesting PAM accesses .....	109
Attesting departments .....	110
Application role attestation .....	110
Business role attestation .....	111
Attesting system roles .....	112
Attesting locations .....	113
Attesting system roles .....	114
Attesting memberships in system entitlements .....	114
Attesting memberships in application roles .....	117
Attestation of memberships in business roles .....	118
Attesting assignment of memberships in system roles .....	120
Attesting device owners .....	121
Attesting system entitlement owners .....	122
Attesting system entitlement owners (initial) .....	122
Attesting user accounts .....	123
Attesting system entitlements .....	124
Attesting assignment of system entitlement to departments .....	125
Attesting assignment of system entitlement to business roles .....	126
Attestation of system entitlement assignments to cost centers .....	127
Attestation of system entitlement assignments to locations .....	128
Attesting assignment of system role assignment to departments .....	130
Attesting assignment of system roles to business roles .....	131
Cost center system role assignment attestation .....	132

Attesting assignment of system entitlements to locations ..... 133

Attesting assignments to system roles .....134

**About us .....136**

    Contacting us ..... 136

    Technical support resources ..... 136

**Index .....137**

## General tips and getting started

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

**NOTE:** This guide describes the Web Portal with its factory settings. Your version of the Web Portal may be different because your Web Portal may have been customized.

In addition, which Web Portal functionality is available to you is controlled by a role model in the database. This guide describes all the Web Portal functions. If you cannot find one of the functions described here in your Web Portal, it may be due to insufficient permissions. In this case, ask your administrator.

### Tips for using the Web Portal

- Enable JavaScript in your browser for the Web Portal to work.
- A minimum screen resolution of 1280x1024 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.
- Supported browsers:
  - Firefox (release channel)
  - Chrome (release channel)
  - Safari (current version)
  - Microsoft Edge (release channel)

### Detailed information about this topic

- [Logging in and out](#) on page 10
- [Navigation and use](#) on page 12
- [Displaying the address book](#)
- [Managing password questions](#) on page 16
- [Changing passwords](#) on page 18
- [Switching languages](#) on page 19

- [Enabling/disabling email notifications](#) on page 19
- [Report subscriptions management](#) on page 20
- [The user interface layout](#) on page 23

## Logging in and out

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

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

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

### Detailed information about this topic

- [Logging in](#) on page 10
- [Logging in to the Password Reset Portal](#) on page 11
- [Logging off](#) on page 12

## Logging in

Open the Web Portal in a web browser.

### *To log in to the Web Portal*

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

### Related topics

- [Changing passwords](#) on page 18

# Logging in to the Password Reset Portal

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

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

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

## ***To log in to Password Reset Portal using an passcode***

1. Open the Password Reset Portal URL in your web browser.  
The Password Reset Portal opens.
2. On the login page, in the **Authentication** menu, select the **Login with passcode** option.
3. In the **User name** field, enter your user name.
4. In the **Enter characters from the image** field, enter the Captcha Code displayed.  
**TIP:** If you cannot clearly identify the CAPTCHA code displayed, click **Refresh image**. A new CAPTCHA code is then generated.
5. Click **Next**.
6. In the **Passcode** field, enter your passcode.
7. Click **Submit**.

## ***To log in to Password Reset Portal using your password questions***

1. Open the Password Reset Portal URL in your web browser.  
The Password Reset Portal opens.
2. On the login page, in the **Authentication** menu, select the **Log in by answering your password questions** option.
3. In the **User name** field, enter your user name.
4. In the **Enter characters from the image** field, enter the Captcha Code displayed.  
**TIP:** If you cannot clearly identify the CAPTCHA code displayed, click **Refresh image**. A new CAPTCHA code is then generated.
5. Click **Next**.
6. In the fields, enter the appropriate answers to your password questions.
7. Click **Submit**.

### ***To log in to Password Reset Portal using your current password***

1. Open the Password Reset Portal URL in your web browser.  
The Password Reset Portal opens.
2. On the login page, in the **Authentication** menu, select the corresponding authentication method.
3. In the **User name** field, enter your user name.
4. In the **Password** field, enter your personal password.
5. Click **Log in**.


### **Related topics**

- [Logging in](#) on page 10
- [Logging off](#) on page 12

## **Logging off**

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

### ***To log off from Web Portal***

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

Your logoff was successful.

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

## **Navigation and use**

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

### **Detailed information about this topic**

- [Simple navigation](#) on page 13
- [Search](#) on page 14
- [Help](#) on page 15
- [Filtering](#) on page 16

# Simple navigation

## Simple commands

**Table 1: Overview of simple commands**

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

**NOTE:** Take into account that not all browsers behave the same. The shortcuts described here were set up with the help of Internet Explorer 9.

## Go to the home page

**Table 2: Overview of key combinations for navigating**

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

## Simple elements

**Table 3: Overview of the controls used**

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

Check box	Use the Tab key to navigate to the required check box and press Space to enable the check box.
Option	Use the Tab key to navigate to the required list of options. Use the arrow keys to choose between the different options. Use Tab to leave the list of options.

## Installed controls

**Table 4: Overview of other controls**

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

## Search

Many of the pages provide a function to search for objects in context.

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

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

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

Example	Description
Sam User	Finds Sam User but not Sam Identity. Search results must contain all of the separate terms in the query. A logical <b>AND</b> is used.
Sam OR Identity	Finds Sam User and Pat Identity. Placing <b>OR</b> between the search terms acts as a logical OR operator. The results of this search contain at least one of the two search terms.
Sam NOT User	Finds Sam Identity but not Sam User. The results of this search do not contain the term that comes after <b>NOT</b> .
U*	Finds User1 and User2. The <b>*</b> functions as a wildcard for any number of characters to complete the term.
Use?	Finds User but not User1. The <b>?</b> functions as a wildcard for a single character to complete the term.
"Sam User"	Provides results in which the search terms <b>Sam</b> and <b>User</b> follow one another.

Example	Description
	Results of this search contain the string in quotes as phrase.
Sam User~	<p>Finds Sam User and also other similar results. A tilde ~ after the search term indicates that the search should also find similar results. This means that incorrectly spelled terms can be found, as well.</p> <p>You can specify the level of similarity by adding a number between <b>0</b> and <b>1</b> (with decimal point) after the tilde ~. The higher the number, the more similar the results.</p>

### Detailed information about this topic

- [Context searching](#) on page 15

## Context searching

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

### To run a context search

1. In the 🔍 **Search** field, enter the search term.  
Any results matching your query are displayed.
2. (Optional) To clear the search, click ✕ (**Reset filter**).

## Help

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

### Detailed information about this topic

- [Using the help](#) on page 15

## Using the help

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

### To call up help in the Web Portal

- In the header, click ? (**Help**) > .  
The One Identity Manager Web Designer Web Portal User Guide opens as online help.

# Filtering

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

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

## *To use a filter*

1. On the page with the filter function, click ▼ (**Filter**).
2. In the menu, enable the filter that you want to apply.
3. (Optional) To reset the filter, click ▼ (**Filter**) and then **Clear filters**.

# Displaying the address book

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

## *To display the address book*

1. In the header, click 👤 (**Profile**) > **Address Book**.  
This displays the address book and all identities.
2. (Optional) On the **Address Book** page, click an identity.  
In the **View Identity Details** pane, you are provided with further details about the identity.

# Managing password questions

If you forget your password, you can change it at any time in the Web Portal (see [Changing passwords](#) on page 18). To do this, you need to define individual questions that only you can answer.

If your password questions are incorrectly answered, you are locked out. You can reset locked password questions at any time.

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

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


## Detailed information about this topic

- [Creating password questions](#)
- [Editing password questions](#)
- [Deleting password questions](#)

# Creating password questions

You can create new password questions.


### *To create new a password question*

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page click the **Password Questions** tab.
3. On the **Password Questions** tab, click **Create password question**.
4. In the **Create Password Question** pane, enter the following:
  - **Question:** Enter your question.
  - **Answer:** Enter the answer to your question (above).
  - **Repeat answer:** Enter the answer to your question again.
5. Click **Save**.

# Editing password questions

You can edit existing password questions.


### *To edit a password question*

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page click the **Password Questions** tab.
3. In the **Password Questions** tab, click the password question you want to edit.
4. Click **Edit**.
5. Specify the following:
  - **Question:** Enter your question.
  - **Answer:** Enter the answer to your question (above).
  - **Repeat answer:** Enter the answer to your question again.
6. Click **Save**.

# Deleting password questions

You can delete existing password questions.

## ***To delete a password question***

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page click the **Password Questions** tab.
3. On the **Password Questions** tab, click the password question you want to delete.
4. Click **Delete**.
5. In the **Delete password question** dialog, confirm the prompt with **Yes**.

# Changing passwords

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

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

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

## **Step 1: Log in to the Password Reset Portal**

Log in to the Password Reset Portal using a passcode, by answering your password questions, or with your current password (see [Logging in to the Password Reset Portal](#) on page 11).

## **Step 2: Change password**

After you have logged in on the Password Reset Portal (see [Step 1: Log in to the Password Reset Portal](#) on page 18), you can change your central password or the passwords of user accounts to which you have access.

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

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

### ***To change the central password***

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

The central password is reset.

### **Related topics**


- [Managing password questions](#) on page 16

## **Switching languages**

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

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

### ***To change the language of the Web Portal***

1. In the header, click  (**Profile**) > **My profile**.
2. On the **Profile Settings** page, click **Main Data**.
3. In the **Language** menu, select the language that you want to use for the Web Portal.
4. In the **Language for value formatting** menu, select the language you want to use for date and number formats.


For example, German dates are displayed in the format DD.MM.JJJJ (**24.12.2020**) and in English US format MM/DD/JJJJ (**12/24/2020**).

5. Click **Save**.

## **Enabling/disabling email notifications**

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

### ***To enable/disable email notifications***

1. In the header, click  (**Profile**) > **My profile**.
2. On the **Profile Settings** page, click the **Email Notifications** tab.

3. Perform one of the following tasks:
  - To enable notifications, select the check box next to the event that you want to notified about.
  - To disable notifications, deselect the box next to the event that you do not want to notified about any longer.
4. Click **Save**.

## Report subscriptions management

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

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



### Detailed information about this topic

- [Subscribing to reports](#) on page 20
- [Editing report subscriptions](#) on page 21
- [Sending reports from report subscriptions](#) on page 22
- [Unsubscribing reports](#) on page 22

## Subscribing to reports

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

### To add a subscription

1. In the header, click  (**Profile**) > **My report subscriptions**.  
In the header, click  (**Profile**) > **My profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.
3. On the **Report Subscriptions** tab, click **Add subscription**.  
On the **Report Subscriptions** page, click **Add subscription**.
4. In the **Add Report Subscription** pane, in the list, click the report that you want to subscribe to.  

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

6. In the **Configure subscription** step, specify the following subscription settings:
  - **Subscription:** Enter the subscription's name.
  - **Schedule:** Select how often you want to receive the report (once a week, for example).
  - **Format (email attachment):** Select which format you want to receive the report in. The report is sent in this format as a file attachment in an email.
  - **Parameter:** (Optional) Specify other report specific settings. These settings might vary depending on what report you use.
7. Click **Next**.
8. In the **Add additional subscribers** step, in the **Additional subscribers** list, click the identities that will also receive this report.


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

**TIP:** To remove a subscriber, in the **Selected subscribers** list, click **✕ (Remove)** next to the corresponding identity. To remove all subscribers, in the **Selected subscribers** list, click **Remove all**.
9. Click **Next**.
10. In the **Check and create subscription** step, check your data and change them if necessary by clicking on the respective step.
11. Click **Create**.

## Editing report subscriptions

You can edit your existing report subscriptions.

### *To edit a report subscription*

1. In the header, click  (**Profile**) > **My profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.
3. On the **Report Subscriptions** page, click **Edit** next to the report subscription that you want to edit.
4. In the details pane, under **Subscription Details**, edit the following report subscription settings:
  - **Subscription:** Enter the report subscription's name.
  - **Report:** Select the report that you want to subscribe to.
  - **Schedule:** Select how often you want to receive the report (once a week, for example).
  - **Format (email attachment):** Select which format you want to receive the report in. The report is sent in this format as a file attachment in an email.

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




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

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

## Sending reports from report subscriptions

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




### *To send a report*

1. In the header, click  (**Profile**) > **My profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.
3. On the **Report Subscriptions** tab, perform the following:  
On the **Report Subscriptions** page, perform the following:
  - To send the report, click  (**Actions**) > **Send report to me** next to the subscription of the report that you want to send.
  - To send the report to all subscribers, click  (**Actions**) > **Send report to all subscribers** next to the subscription of the report you want to send.

## Unsubscribing reports

You can unsubscribe reports.

### *To unsubscribe a report*

1. In the header, click  (**Profile**) > **My profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.
3. On the **Report Subscriptions** tab, click  (**Actions**) > **Unsubscribe** next to the report subscription that you want to end.  
On the **Report Subscriptions** page, click  (**Actions**) > **Unsubscribe** next to the report subscription that you want to end.
4. In the **Unsubscribe Report** dialog, confirm the prompt with **OK**.

# The user interface layout

The Web Portal user interface is divided into several sections:

## Top - header

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

## Top – menu bar

The [menu bar](#) is displayed horizontally in the upper part of the screen and provides different menus and submenus.

## Work area

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

## Detailed information about this topic

- [Home](#) on page 23
- [Header](#) on page 23
- [Menu bar](#) on page 24

## Home

Open the home page by clicking the company logo.



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

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

## Header

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

**Table 6: Functions in the header**

 Profile	<p>Use these menu items to:</p> <ul style="list-style-type: none"><li>• View your personal data with memberships, responsibilities, and entitlements and to edit setting (for example, your <a href="#">Password questions</a>)</li><li>• <a href="#">Display</a> your company's address book</li><li>• <a href="#">Log off</a></li><li>• <a href="#">Change</a> the language</li><li>• <a href="#">Enable/disable</a> email notifications</li><li>• <a href="#">Manage</a> report subscriptions</li></ul>
 Help	<p>This menu includes <a href="#">online help</a>, contact to customer service and information about the connection and the product.</p> <p>Use <b>Documentation</b> to open the context-sensitive help. The help contains the entire contents of the Web Portal User Guide.</p> <p>Here you can <a href="#">open</a> the help. The help contains the entire contents of the Web Portal User Guide.</p>

## Menu bar

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

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

### ***To open a menu***

1. Click a menu in the menu bar.  
This expands the menu and shows more menu items.
2. Click a menu item.

## Requests

Requests account for the core functionality of the Web Portal. For example, if you require access to a system or device, request it as though you were using a traditional web shop.

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

You can apply the following requests:

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

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

- Your request is forwarded to an identity for approval (see [Pending requests](#) on page 42).
- You are notified whether your request is granted or denied.

### Detailed information about this topic

- [Requesting products](#) on page 26
- [Saved for Later list](#) on page 39
- [Pending requests](#) on page 42
- [Displaying request history](#) on page 50
- [Canceling requests](#) on page 51
- [Renewing products with limit validity periods](#) on page 51
- [Unsubscribing products](#) on page 53
- [Displaying approvals](#) on page 54

# Requesting products

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

You can complete a request in three steps:

1. Add the desired product to your shopping cart (see [Adding products to the shopping cart](#) on page 26).
2. Verify the shopping cart and amend the product requests as required (see [Managing products in the shopping cart](#) on page 27).
3. Submit the request (see [Submitting requests](#) on page 33).

## Detailed information about this topic

- [Adding products to the shopping cart](#) on page 26
- [Managing products in the shopping cart](#) on page 27
- [Submitting requests](#) on page 33
- [Requesting products on the Saved for Later list](#) on page 40
- [Displaying and requesting other identity's products](#)
- [Requesting for other identities or subidentities](#) on page 36
- [Requests for Active Directory groups](#)

# Adding products to the shopping cart

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

## *To add products to the shopping cart*

1. In the menu bar, click **Requests > New request**.  
This opens the **New Request** page and displays all the available products.
2. (Optional) To filter which products are displayed, perform one of the following actions:
  - In the search field, enter the name of a product you want to look for.
  - Click **Show products from service category** and then select the service category containing the products you want to display.

The relevant products are displayed.

**TIP:** To change the service category you have selected, click **✕ (Delete filter)** next to the selected service category and then select another service category

using **Show products from service category**.

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

To summarize the main and child categories in a list, enable the **Include child categories** option.

3. Perform one of the following tasks:

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

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

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

- In the list view (☰)
- Add a product to the shopping cart: Next to the product with the product you want to request, click **Add to cart**.
- Add multiple products to the shopping cart: Select the check boxes next to the products you want to request and click **Add to cart** below the list.

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

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

This opens the **Shopping Cart** page. Now, you can check the request and, if necessary, add to each product request (see [Managing products in the shopping cart](#) on page 27). Then send the request (see [Submitting requests](#) on page 33).

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

## Related topics

- [Managing products in the shopping cart](#) on page 27
- [Submitting requests](#) on page 33

# Managing products in the shopping cart

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 26), you can delete individual product requests from the cart, add more details to them, or perform other actions.

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

### ***To manage products in the shopping cart***

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, edit the shopping cart.  
You can perform the following actions:
  - Remove products from the shopping cart (see [Removing products from the shopping cart](#) on page 29)
  - Define the validity of the products (see [Setting the validity period of products in your shopping cart](#) on page 30)
  - Change the priority of the requests (see [Specifying the priority of products in your shopping cart](#) on page 30)
  - Enter reasons for the requests (see [Giving reasons for requests](#) on page 31)
  - Check the shopping cart for invalid products and remove them (see [Checking the shopping cart](#) on page 31)
  - Request products for multiple identities (see [Requesting products in the shopping cart for multiple identities](#) on page 32)
  - Place products on the Saved for Later list (see [Saving products for later](#) on page 39)
  - Show the Saved for Later list (see [Displaying Saved for Later list](#) on page 40)
3. Ensure you only have requests that you really want to submit in your cart.  
Now you can send your request (see [Submitting requests](#) on page 33).

### **Related topics**

- [Adding products to the shopping cart](#) on page 26
- [Submitting requests](#) on page 33
- [Saved for Later list](#) on page 39

## **Displaying the shopping cart**

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 26), you can view all the products in your shopping cart along with their details.

### ***To display the products in your shopping cart***

1. In the menu bar, click **Requests > Shopping cart**.  
This opens the **Shopping Cart** page.
2. Now you can [add](#) more products to your shopping cart, [set](#) additional options for products in the shopping cart, or [submit](#) the request.

### **Related topics**

- [Adding products to the shopping cart](#) on page 26
- [Submitting requests](#) on page 33

## **Removing products from the shopping cart**

After adding added products to your shopping cart (see [Adding products to the shopping cart](#) on page 26), you can remove them again.

### ***To remove products from the shopping cart***

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, click **Remove from cart** next to the product that you do not want to request anymore.
3. In the **Remove Product From Cart** dialog, confirm the prompt with **Yes**.  
Now you can [add](#) more products to your shopping cart, [set](#) additional options for products in the shopping cart, or [submit](#) the request.

### ***To remove multiple products from the shopping cart***

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you do not want to request anymore.
3. Click **⋮ (Actions) > Remove selected**.
4. In the **Remove Selected Products From Cart** dialog, confirm the prompt with **Yes**.  
Now you can [add](#) more products to your shopping cart, [set](#) additional options for products in the shopping cart, or [submit](#) the request.

### ***To remove all products from the shopping cart***

- Delete the shopping cart. For more information, see [Deleting shopping carts](#) on page 33.

## Related topics

- [Adding products to the shopping cart](#) on page 26
- [Submitting requests](#) on page 33

## Setting the validity period of products in your shopping cart

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 26), you can set their validity period. Once a product's validity period has expired, it can no longer be used.

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

**TIP:** You can renew the validity of a currently assigned product. For more information, see [Renewing products with limit validity periods](#) on page 51.

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

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, in the list, click **Edit** next to the product whose validity period you want define.
3. In the details pane, in the **Valid from** field, specify from when the product is valid.
4. In the **Valid until** field, specify until when the product is valid.
5. Click **Save**.

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

## Related topics

- [Adding products to the shopping cart](#) on page 26
- [Submitting requests](#) on page 33

## Specifying the priority of products in your shopping cart

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 26), you can specify their priority. The priority allows approvers to quickly identify how important a product request is.

### ***To specify the priority of a product in the shopping cart***

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, click **Edit** next to the product whose priority you want define.
3. In the details pane, in the **Priority** menu, select the priority.
4. Click **Save**.

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

### **Related topics**

- [Adding products to the shopping cart](#) on page 26
- [Submitting requests](#) on page 33

## **Giving reasons for requests**

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 26), you can give reasons for requesting them. A reason can help approvers make their approval decisions.

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

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

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

### **Related topics**

- [Adding products to the shopping cart](#) on page 26
- [Submitting requests](#) on page 33

## **Checking the shopping cart**

When you send a request, it is automatically checked to see if it contains invalid products. You can also [run](#) this check before you submit the request. If necessary, you will be shown why specific product requests are invalid.

### ***To check your shopping cart for invalid products***

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

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

If invalid products are found, an appropriate message appears in the **Check result** column next to the invalid product.

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

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

### **Related topics**

- [Adding products to the shopping cart](#) on page 26
- [Submitting requests](#) on page 33

## **Requesting products in the shopping cart for multiple identities**

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 26), you can request the products in your shopping cart for other identities as well.

### ***To request a product in the shopping cart for multiple identities***

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, click **Edit** next to the product that you want to request for other identities.
3. In the details pane, click **Actions > Request for multiple identities**.
4. In the **Request for Multiple Identities** pane, select the check boxes next to the identities you want to request the product for.
5. Click **Apply**.
6. Close the details pane.

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

## Related topics

- [Requesting for other identities or subidentities](#) on page 36
- [Adding products to the shopping cart](#) on page 26
- [Submitting requests](#) on page 33

## Deleting shopping carts

You can clear your shopping cart at any time.

### *To delete your shopping cart*

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, click **⋮ (Actions) > Delete shopping cart**.
3. In the **Delete Shopping Cart** dialog, confirm the prompt with **Yes**.

## Related topics

- [Removing products from the shopping cart](#) on page 29
- [Adding products to the shopping cart](#) on page 26

## Submitting requests

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 26), and edited and, if necessary, checked the request (see [Managing products in the shopping cart](#) on page 27), you can submit your shopping cart.

### *To submit your requests*

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

This checks, submits, and triggers the request workflow.

**TIP:** To check the request's validity before you submit the request, click **⋮ (Actions) > Check shopping cart**. You can solve most problems of invalid product requests in the shopping cart by removing the problem product from the shopping cart (see [Checking the shopping cart](#) on page 31 and [Removing products from the shopping cart](#) on page 29).

## Related topics

- [Adding products to the shopping cart](#) on page 26
- [Managing products in the shopping cart](#) on page 27

- [Checking the shopping cart](#) on page 31
- [Removing products from the shopping cart](#) on page 29

## Displaying and requesting other identity's products

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

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

### Related topics

- [Requesting products in the shopping cart for multiple identities](#) on page 32
- [Requesting for other identities or subidentities](#) on page 36

## Requesting products through reference users

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

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

1. In the menu bar, click **Requests > New request**.
2. On the **/New Request** page, click **(Actions) > Select a reference user**.
3. In the **Select Reference User** dialog, click **Assign** next to the identity whose products you also want to request.  
  
This opens the **New Request - By Reference User** page that, on the **Products** and **Organizational Structures** tabs, lists the requests, memberships, and entitlements of the selected identity.
4. Add the products that you want to save for later, to the shopping cart (see [Adding products to the shopping cart](#) on page 26).
5. On the **My Shopping Cart** page, click **Submit**.

**TIP:** You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 27.

## Related topics

- [Requesting products through peer groups](#) on page 35
- [Managing products in the shopping cart](#) on page 27

# Requesting products through peer groups

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

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

## *To request other identities' products*

1. In the menu bar, click **Requests > New request**.
2. (Optional) If you want to make a request for another identity or check which products have been requested by their peer group, proceed as follows:
  - a. On the **New Request** page, click **Change** next to the **Recipient** field.
  - b. In the **Edit Property** pane, in the list, select the check boxes next to the identity you want to request products for.

**NOTE:** The list may contain a maximum of one identity. To remove an identity from the list, clear the check box in front of the corresponding identity.

- c. Click **Apply**.
3. On the **New Request** page, click **(Actions) > Show products other identities requested**.

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

4. Add the products that you want to save for later, to the shopping cart (see [Adding products to the shopping cart](#) on page 26).
5. On the **My Shopping Cart** page, click **Submit**.

**TIP:** You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 27.

## Related topics

- [Requesting products through reference users](#) on page 34
- [Managing products in the shopping cart](#) on page 27

# Requesting for other identities or subidentities

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

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

**TIP:** You can also request products for other identities directly from the shopping cart. For more information, see [Requesting products in the shopping cart for multiple identities](#) on page 32.

## **To request products for other identities**

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, click **Change** next to the **Recipient** field.
3. In the **Edit Property** pane, in the list, select the check boxes next to the identities you want to request products for.  
**TIP:** To remove an identity from the recipient list, deselect the check box next to the identity.
4. Click **Apply**.
5. Add the products to the shopping cart (see [Adding products to the shopping cart](#) on page 26) that you want to request for the selected identities.
6. (Optional) Edit the shopping cart (see [Managing products in the shopping cart](#) on page 27).
7. Submit the request (see [Submitting requests](#) on page 33).

## **Related topics**

- [Requesting products in the shopping cart for multiple identities](#) on page 32

# Requests for Active Directory groups

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

## **Detailed information about this topic**

- [Requesting new Active Directory groups](#) on page 37
- [Requesting changes to Active Directory groups](#) on page 38
- [Requesting deletion of Active Directory groups](#) on page 39

# Requesting new Active Directory groups

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

## *To request a new Active Directory group*

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, click **Show products from service category**.
3. In the **Service category** pane, click the **Active Directory groups** service category.
4. Perform one of the following actions:
  - To request a new Active Directory security group, click the **New Active Directory security group** tile.
  - To request a new Active Directory distribution group, click the **New Active Directory distribution group** tile.
5. Click **Add to cart**.
6. In the **Request Details** pane, specify additional information about the new group:
  - **Name:** Enter a name for the group.
  - **Group scope:** Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can select one of the following group scopes:
    - **Global group:** Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group's domain.
    - **Local:** Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.
    - **Universal:** Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
  - **Container:** Click **Assign** and select a container for the group.
7. Click **Apply**.
8. Click **Submit**.

**TIP:** You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 27.
9. On the **Shopping Cart** page, click **Submit**.

## Related topics

- [Approving pending requests from newly created Active Directory groups](#) on page 44

# Requesting changes to Active Directory groups

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

### *To change an Active Directory group*

1. In the menu bar, click **Requests > New request**.
2. On the **Request** page, click **Show products from service category**.
3. In the **Service category** pane, click the **Active Directory groups** service category.
4. Click the **Modify Active Directory group** tile.
5. Click **Add to cart**.
6. In the **Request Details** pane, in the **Active Directory group** menu, select the Active Directory group that you want to change.
7. (Optional) In the **Group scope** menu, select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can select one of the following group scopes:
  - **Global group**: Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group's domain.
  - **Local**: Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.
  - **Universal**: Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
8. (Optional) In the **Type** menu, select the type of Active Directory group (security or distribution group).
9. Click **Apply**.
10. Click **Submit**.

**TIP:** You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 27.
11. On the **Shopping Cart** page, click **Submit**.

# Requesting deletion of Active Directory groups

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

## *To delete an Active Directory group*

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, click **Show products from service category**.
3. In the **Service category** pane, click the **Active Directory groups** service category.
4. Click the **Delete Active Directory Group** tile.
5. Click **Add to cart**.
6. In the **Request Details** pane, in the **Active Directory group to delete** menu, select the Active Directory group that you want to delete.
7. Click **Apply**.
8. Click **Submit**.

**TIP:** You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 27.

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

# Saved for Later list

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

## Detailed information about this topic

- [Saving products for later](#) on page 39
- [Displaying Saved for Later list](#) on page 40
- [Requesting products on the Saved for Later list](#) on page 40
- [Removing products from the Saved for Later list](#) on page 41
- [Deleting the Saved for Later list](#) on page 42

# Saving products for later

If you do not want to request products immediately but at a later date, you can save the products on the Saved for Later list. You can access your Saved for Later list at any time,

move products from it into your shopping cart, and request them (see [Requesting products on the Saved for Later list](#) on page 40).

***To add products to your Saved for Later list.***

1. Add the products that you want to save for later, to the shopping cart (see [Adding products to the shopping cart](#) on page 26).
2. In the menu bar, click **Requests > Shopping cart**.
3. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you want to save for later.
4. Click **⋮ (Actions) > Move to Saved for Later list**.

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

**Related topics**

- [Managing products in the shopping cart](#) on page 27

## Displaying Saved for Later list

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

***To display your Saved for Later list***

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

**Related topics**

- [Managing products in the shopping cart](#) on page 27

## Requesting products on the Saved for Later list

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

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

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, perform one of the following actions:
  - If there are products in the shopping cart, click **⋮ (Actions) > View Saved for Later**.
  - If the shopping cart is empty, click **View Saved for Later list**.
3. On the **Saved for Later** page, select the check boxes in front of the products in the list that you want to request or add to the shopping cart.
4. Click **⋮ (Actions) > Move to shopping cart**.  
This moves the products and all their settings to your shopping cart.
5. On the **Shopping Cart** page, click **Submit**.

**TIP:** You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 27.

**Related topics**

- [Managing products in the shopping cart](#) on page 27
- [Submitting requests](#) on page 33

## Removing products from the Saved for Later list

You can remove products from your Saved for Later list. To delete the entire Saved for Later list, see [Deleting the Saved for Later list](#) on page 42.

***To remove a product from your Saved for Later list***

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, perform one of the following actions:
  - If there are products in the shopping cart, click **⋮ (Actions) > View Saved for Later**.
  - If the shopping cart is empty, click **View Saved for Later list**.
3. On the **Saved for Later** page, click **Remove from list** next to the product you want to remove from the Save for Later list.
4. In the **Remove Product From Saved For Later List** dialog, confirm the prompt with **Yes**.

### ***To remove multiple products from your Saved for Later list***

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

### **Related topics**

- [Managing products in the shopping cart](#) on page 27

## **Deleting the Saved for Later list**

You can delete your Saved for Later list. For more information about removing individual products, see [Removing products from the Saved for Later list](#) on page 41.

### ***To delete your Saved for Later list***

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

### **Related topics**

- [Managing products in the shopping cart](#) on page 27

## **Pending requests**

Many requests go through a manual approval process in order to ensure the correct assignment of products. If the request requires approving or denying, the request classifies as pending and as approver you can make the approval decision. If you need more

information to make an approval decision, you can submit an inquiry, add more approvers, or reroute the request.

### Detailed information about this topic

- [Displaying pending requests](#) on page 43
- [Approving and denying requests](#) on page 43
- [Appointing other approvers for pending requests](#) on page 45
- [Rejecting request approval](#) on page 49

## Displaying pending requests

If you are the approver of certain products and identities request these products, you can display the requests. Then you can make approval decisions about the pending requests (see [Approving and denying requests](#) on page 43).

### *To display pending requests*

1. In the menu bar, click **Requests > Pending requests**.  
This opens the **Pending Requests** page.
2. (Optional) To display details of a pending request, click **Details** next to the request whose details you want to see.

## Approving and denying requests

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

### *To make an approval decision about a pending request*

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

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

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

- a. In the **Reason for your decision** field, select a standard reason for your approval decision.
- b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

4. (Optional) To specify a validity period for the requested product, perform the following actions:
  - a. In the **Valid from** field, specify from when the products are is valid.
  - b. In the **Valid until** field, specify until when the product is valid.
5. Click **Save**.

## Approving pending requests from newly created Active Directory groups

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

### *To approve a request to create a new Active Directory group*

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click **Approve** next to the request for a new Active Directory group.
3. In the **Approve Request** section, enter additional information about the new group:
  - **Name:** Enter a name for the group.
  - **Group scope:** Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can select one of the following group scopes:
    - **Global group:** Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group's domain.
    - **Local:** Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.
    - **Universal:** Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
  - **Container:** Click **Assign/Change** and select a container for the group.

4. (Optional) To specify a validity period for the Active Directory group, perform the following actions:
    - a. In the **Valid from** field, specify as from when the Active Directory groups are valid.
    - b. In the **Valid until** field, specify until when the Active Directory groups are valid.
  5. (Optional) Perform one of the following actions:
    - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
    - b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.
- TIP:** By giving reasons, your approvals are more transparent and support the audit trail.
- NOTE:** For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
6. Click **Save**.

## Related topics

- [Requesting new Active Directory groups](#) on page 37

# Appointing other approvers for pending requests

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

- **Reroute approval**  
You give the task of approving to another approval level (see [Rerouting approvals of pending requests](#) on page 46).
- **Appoint additional approver**  
You can give an another identity the task of approving (see [Appointing additional approvers to pending requests](#) on page 46). The additional approver must make an approval decision in addition to the other approvers.  
The additional approver can reject the approval and return it to you (see [Rejecting request approval](#) on page 49).  
You can withdraw an additional approver. For example, if the other approver is not available.
- **Delegate approval**  
You delegate the task of approving to another approval level (see [Delegating approvals of pending requests to other identities](#) on page 48). This identity is added as approver in the current approval step and makes approval decisions on your

behalf.

The new approver can reject the approval and return it to you (see [Rejecting request approval](#) on page 49).

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

## Rerouting approvals of pending requests

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

### *To reroute an approval*

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

### *To reroute multiple approvals*

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

## Appointing additional approvers to pending requests

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

### ***To add an additional approver***

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, in the list, click **Details** next to the request to which you want to add an additional approver.
3. In the **View Request Details** pane, click **Add approver**.
4. In the **Add Additional Approver** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.
5. In the **Reason for your decision** field, select a standard reason for adding an additional approver.
6. Click **Save**.

### ***To add an additional approver to multiple requests***

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, in the list, select the check boxes next to the requests to which you want to add an additional approver.
3. Click **⋮ (Actions) > Add approver**.
4. In the **Add Additional Approver** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.
5. In the **Reason for your decision** field, select a standard reason for adding an additional approver.
6. Click **Save**.

### **Related topics**

- [Removing additional approvers of pending requests](#) on page 47

## **Removing additional approvers of pending requests**

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

### ***To withdraw a request's additional approver***

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click **Details** next to the request to which you added an additional approver.
3. In the **View Request Details** pane, click **Withdraw additional approver**.
4. In the **Withdraw Additional Approver** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.
5. Click **Save**.

### ***To withdraw additional approver from multiple requests***

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, in the list, select the check boxes next to the requests to which you added an additional approver.
3. Click **⋮ (Actions) > Withdraw additional approver**.
4. In the **Withdraw Additional Approver** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.
5. Click **Save**.

### **Related topics**

- [Appointing additional approvers to pending requests](#) on page 46

## **Delegating approvals of pending requests to other identities**

You can delegate an approval decision about a request to another identity. You can revoke this action in the approval history (see [Withdrawing delegations from pending requests](#) on page 49).

### ***To delegate an approval***

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click **Details** next to the request whose approval decision you want to delegate to another identity.
3. In the **View Request Details** pane, click **Delegate approval**.
4. In the **Delegate approval**, in the **Delegate to** menu, select the identity to which you want to delegate the approval.
5. In the **Reason for your decision** field, enter a reason for the delegation.
6. Click **Save**.

### ***To delegate approval of multiple requests***

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, in the list, select the check boxes next to the requests whose approval you want to delegate to another identity.
3. Click **⋮ (Actions) > Delegate approval**.
4. In the **Delegate approval**, in the **Delegate to** menu, select the identity to which you want to delegate the approval.
5. In the **Reason for your decision** field, enter a reason for the delegation.
6. Click **Save**.

## Related topics

- [Withdrawing delegations from pending requests](#) on page 49

## Withdrawing delegations from pending requests

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

### *To withdraw an approval delegation*

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click **Details** next to the request with the approval delegation you want to withdraw.
3. In the **View Request Details** pane, click **Withdraw delegation**.
4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegation.
5. Click **Save**.

### *To withdraw multiple delegations from approvals*

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, in the list, select the check boxes next to the requests whose approval delegations you want to withdraw.
3. Click **⋮ (Actions) > Withdraw delegation**.
4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegations.
5. Click **Save**.

## Related topics

- [Delegating approvals of pending requests to other identities](#) on page 48

## Rejecting request approval

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

### ***To reject an approval***

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click **Details** next to the request that you do not want to make an approval decision about.
3. In the **View Request Details** pane, click **Reject approval**.
4. In the **Reject Approval**, in the **Reason for your decision** pane, enter a reason for the rejecting.
5. Click **Save**.

### ***To reject approval of multiple requests***

1. In the menu bar, click **Requests > Pending requests**.
  2. On the **Pending Requests** page, in the list, select the check boxes next to the requests that you do not want to make an approval decision about.
  3. Click **⋮ (Actions) > Reject approval**.
  4. In the **Reject Approval**, in the **Reason for your decision** pane, enter a reason for the rejecting.
  5. Click **Save**.
- [Appointing additional approvers to pending requests](#) on page 46

## **Displaying request history**

You can display the request history to obtain an overview of all the products that you have requested for yourself or other identities, or to see the status of a current request.

### ***To display the request history***

1. In the menu bar, click **Requests > Request History**.  
This opens the **Request History** page.
2. (Optional) To control which requests are displayed, click **▼ (Filter)** (see [Filtering](#) on page 16). For example, this allows you to show just pending requests (no approval decision yet made).
3. (Optional) To display details of a request, click **Details** next to the request whose details you want to see.

### **Related topics**

- [Canceling requests](#) on page 51
- [Renewing products with limit validity periods](#) on page 51
- [Unsubscribing products](#) on page 53

# Canceling requests

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

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

## **To cancel a request**

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click **▼ (Filter)**.
3. In the filter context menu, check the **Pending** box.
4. (Optional) To control which requests are displayed, click **▼ (Filter)** (see [Filtering](#) on page 16). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to cancel a request of another identity, in the **🔍 Search** field, enter the identity's name.
6. Click **Details** next to the request you want to cancel.
7. In the **View Request Details** pane, click **Cancel request**.
8. In the **Cancel Request** pane, perform the following actions:
  - a. In the **Reason for your decision** field, enter a reason for the cancellation.
  - b. Click **Save**.

## **Related topics**

- [Requesting products](#) on page 26
- [Displaying request history](#) on page 50
- [Renewing products with limit validity periods](#) on page 51
- [Unsubscribing products](#) on page 53

# Renewing products with limit validity periods

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

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

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

### ***To renew a product's validity period***

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, check the **Active** box.
4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see [Filtering](#) on page 16). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to renew a product of another identity, in the 🔍 **Search** field, enter the identity's name.
6. Next to the product that you want to renew, click **Details**.
7. In the **View Request Details** pane, click **Renew product**.
8. In the **Renew Product** pane, perform the following actions:
  - a. In the **Renewal date** field, enter the renewal date for the product. If the field is empty the product has unlimited availability.
  - b. In the **Reason for your decision** field, enter a reason for the renewal.
  - c. Click **Save**.

### ***To renew the validity period of multiple products***

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, check the **Active** box.
4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see [Filtering](#) on page 16). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to renew products of another identity, in the 🔍 **Search** field, enter the identity's name.
6. Select the check boxes next to the products you want to renew.
7. Click ⋮ (**Actions**) > **Renew product**.
8. In the **Renew Product** pane, perform the following actions:
  - a. In the **Renewal date** field, enter the renewal date for the products. If the field is empty the products have unlimited availability.
  - b. In the **Reason for your decision** field, enter a reason for the renewal.
  - c. Click **Save**.

### **Related topics**

- [Setting the validity period of products in your shopping cart](#) on page 30
- [Canceling requests](#) on page 51
- [Unsubscribing products](#) on page 53

# Unsubscribing products

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

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

## *To unsubscribe a product*

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, check the **Active** box.
4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see [Filtering](#) on page 16). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to unsubscribe a product of another identity, in the 🔍 **Search** field, enter the identity's name.
6. In the list, click **Details** next to the product that you want to unsubscribe.
7. In the **View Request Details** pane, click **Unsubscribe product**.
8. In the **Unsubscribe Product** pane, perform the following actions:
  - a. In the **Unsubscribed as from** field, enter the date for unsubscribing the product. If you leave this field empty, the product is unsubscribed once you have clicked **Saved**.
  - b. In the **Reason for your decision** field, enter a reason for unsubscribing.
  - c. In the **Additional comments about your decision** field, enter extra information about unsubscribing.
  - d. Click **Save**.

## *To unsubscribe multiple products*

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, check the **Active** box.
4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see [Filtering](#) on page 16). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to unsubscribe products of another identity, in the 🔍 **Search** field, enter the identity's name.
6. In the list, select the check boxes next to the products you want to unsubscribe.
7. Click ⋮ (**Actions**) > **Unsubscribe product**.
8. In the **Unsubscribe Product** pane, perform the following actions:

- a. In the **Unsubscribed as from** field, enter the date for unsubscribing the products. If you leave this field empty, the products are unsubscribed once you have clicked **Saved**.
- b. In the **Reason for your decision** field, enter a reason for unsubscribing.
- c. In the **Additional comments about your decision** field, enter extra information about unsubscribing.
- d. Click **Save**.

### Related topics

- [Displaying request history](#) on page 50
- [Renewing products with limit validity periods](#) on page 51
- [Canceling requests](#) on page 51

## Displaying approvals

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

### *To display approvals*

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click **▼ (Filter)**.
3. In the filter context menu, check the **My approvals** box.
4. (Optional) To display request details (for example, the approval workflow or who can make approval decisions about the request), click **Details** next to the request.

### Related topics

- [Withdrawing delegations from pending requests](#) on page 49
- [Removing additional approvers of pending requests](#) on page 47
- [Approving and denying requests](#) on page 43
- [Undoing approvals](#) on page 54

## Undoing approvals

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

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

### ***To undo an approval***

1. In the menu bar, click **Requests > Request History**.
2. (Optional) To control which requests are displayed on the **Request History** page, click **▼ (Filter)** (see [Filtering](#) on page 16). For example, this allows you to show just pending requests (no approval decision yet made).
3. In the list, click **Details** next to the request whose the approval that you want to undo.
4. In the **View Request Details** pane, click **Undo approval decision**.
5. In the **Undo Approval Decision** dialog, perform the following actions:
  - a. In the **Reason for your decision**, enter why you want to undo the approval.
  - b. Click **Save**.

### **Related topics**

- [Displaying approvals](#) on page 54

## Attestation

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. The same workflow is used for attestation and recertification.

There are attestation policies defined for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom. Once attestation starts, attestation cases are created that contain all the necessary information about the attestation objects and the attestor. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

### Detailed information about this topic

- [Sending attestation reminders](#) on page 56
- [Pending attestations](#) on page 57
- [Displaying attestation history](#) on page 66
- [Attestation – Administration](#) on page 66

## Sending attestation reminders

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

- You can send reminders to attestors of attestation cases that belong to certain attestation runs (see [Sending reminders about attestation runs](#) on page 57).

# Sending reminders about attestation runs

If attestors have not yet processed an attestation case, you can send a reminder email to them to remind them about approving it.

## *To send a reminder to all attestors of all attestation runs*

1. In the menu bar, click **Attestation > Attestation runs**.
2. On the **Attestation Policy Runs** page, click **Send reminders for displayed runs**.
3. (Optional) In the **Send Reminder** pane, in the **Message** field, enter the message for the attestor. This message is added to the reminder.
4. Click **Send reminder**.

## *To send a reminder to attestors of a selected attestation run*

1. In the menu bar, click **Attestation > Attestation runs**.
2. On the **Attestation Policy Runs** page, click **Details** next to the attestation run that has the attestors you want to remind.
3. Perform one of the following actions:
  - To send a reminder to all attestors of the attestation run, in the **View Attestation Run Details** pane, click **Send reminder to all attestors**.
  - To send a reminder to specific attestors of the attestation run, in the **View Attestation Run Details** pane, click the **Attestors** tab, select the check boxes in front of the corresponding attestors and click **Send reminder**.
4. (Optional) In the **Send Reminder** pane, in the **Message** field, enter the message for the attestor. This message is added to the reminder.
5. Click **Send reminder**.

# Pending attestations

Attestation policies are run on a schedule and generate attestation cases. As attestor, you can verify attestation cases and make approval decisions. Verifying attestations requires reading reports or manually checking objects that are being attested.

## Detailed information about this topic

- [Displaying pending attestation cases](#) on page 58
- [Granting or denying attestation cases](#) on page 58
- [Appointing other approvers for pending attestation cases](#) on page 59
- [Rejecting approval of attestation cases](#) on page 65

# Displaying pending attestation cases

As attestor, you can see the attestation cases that still require approval. In addition, you can obtain more information about the attestation cases.

## *To display pending attestation cases*

1. In the menu bar, click **Attestation > Pending Attestations**.  
This opens the **Pending Attestations** page.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. (Optional) To show more details of an attestation case, click **Details** next to the attestation case.
4. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
  - a. In the list, click **Details** next to the attestation case.
  - b. In the **View Attestation Case Details** pane, click **Show details** or **Download report**.
5. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
  - a. In the list, click **Details** next to the attestation case.
  - b. In the **View Attestation Case Details** pane, click the **Workflow** tab.

## Related topics

- [Displaying attestation cases of application runs](#) on page 78

# Granting or denying attestation cases

As attestor, you can grant or deny approval for attestation cases under your supervision.

## *To approve an attestation case*

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:

- To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. Perform one of the following actions:
- To approve an attestation case, click **Approve** next to the attestation case.
  - To deny an attestation case, click **Deny** next to the attestation case.
- TIP:** To approve or deny multiple attestation cases, in the list, select the check boxes next to the attestation cases and click **Approve** or **Deny** below the list.
4. (Optional) In the **Approve Attestation Case/Deny Attestation Case** pane, perform the following actions:
- a. In the **Reason for your decision** field, select a standard reason for your approval decision.
  - b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.
- TIP:** By giving reasons, your approvals are more transparent and support the audit trail.
- NOTE:** For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.
5. Click **Save**.
6. (Optional) If the approval requires multi-factor authentication, you are prompted to enter a security code. It may take a few minutes for the prompt to be displayed. Perform one of the following actions:
- Click **Login with the Starling 2FA app** and follow the app instructions on your mobile phone.
  - Click **Send SMS** or **Phone call**, enter the security code, and click **Next**.

## Related topics

- [Displaying attestation cases of application runs](#) on page 78

# Appointing other approvers for pending attestation cases

You can give an additional identity the task of approving an attestation case. To do this, you have the following options:

- Reroute approval  
You give the task of approving to another approval level (see [Rerouting approvals of](#)

[pending attestation cases](#) on page 60).

- **Appoint additional approver**  
You can give another identity the task of approving [Appointing additional approvers to pending attestation cases](#) on page 61). The additional approver must make an approval decision in addition to the other approvers.  
The additional approver can reject the approval and return it to you (see [Rejecting approval of attestation cases](#) on page 65).  
You can withdraw an additional approver. For example, if the other approver is not available.
- **Delegate approval**  
You delegate the task of approving to another approval level (see [Delegating approvals of pending attestation cases to other identities](#) on page 63). This identity is added as approver in the current approval step and makes approval decisions on your behalf.  
The new approver can reject the approval and return it to you (see [Rejecting approval of attestation cases](#) on page 65).  
You can withdraw a delegation and delegate another identity. For example, if the other approver is not available.

## Rerouting approvals of pending attestation cases

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

### *To reroute an approval*

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, click **Details** next to the attestation case whose approval you want to reroute.
4. In the **View Attestation Case Details** pane, click **Reroute approval**.
5. In the **Reroute approval** pane, in the **Select approval level** menu, select the approval level you want to reroute to.
6. (Optional) In the **Reason for your decision** field, enter a reason for rerouting.
7. Click **Save**.

### ***To reroute multiple approvals***

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases whose approvals you want to reroute.
4. Click **⋮ (Actions) > Reroute approval**.
5. In the **Reroute Approval** pane, in the **Select approval level** menu, select the respective approval level to reroute to.
6. (Optional) In the **Reason for your decision** field, enter a reason for rerouting.
7. Click **Save**.

## **Appointing additional approvers to pending attestation cases**

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

### ***To add an additional approver***

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, in the list, click **Details** next to the attestation case to which you want to add an additional approver.
4. In the **View Attestation Case Details** pane, click **Add attestor**.
5. In the **Add Additional Attestor** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.
6. In the **Reason for your decision** field, select a standard reason for adding an additional approver.
7. Click **Save**.

### ***To add an additional approver to multiple attestation cases***

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases to which you want to add an additional approver.
4. Click **⋮ (Actions) > Add attestor**.
5. In the **Add Additional Attestor** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.
6. In the **Reason for your decision** field, select a standard reason for adding an additional approver.
7. Click **Save**.

### **Related topics**

- [Removing additional approvers from pending attestation cases](#) on page 62

## **Removing additional approvers from pending attestation cases**

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

### ***To withdraw an attestation case's additional approver***

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, click **Details** next to the attestation case to which you added an additional approver.
4. In the **View Attestation Case Details** pane, click **Withdraw additional attestor**.

5. In the **Withdraw Additional Attestor** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.
6. Click **Save**.

### ***To withdraw an additional approver from multiple attestation cases***

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases to which you added an additional approver.
4. Click **⋮ (Actions) > Withdraw additional attestor**.
5. In the **Withdraw Additional Attestor** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.
6. Click **Save**.

### **Related topics**

- [Appointing additional approvers to pending attestation cases](#) on page 61

## **Delegating approvals of pending attestation cases to other identities**

You can delegate an approval decision about an attestation case to another identity. You can revoke this action in the attestation history (see [Withdrawing delegations from pending attestation case approvals](#) on page 64).

### ***To delegate an approval***

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, click **Details** next to the attestation case whose approval decision you want to delegate to another identity.

4. In the **View Attestation Case Details** pane, click **Delegate approval**.
5. In the **Delegate approval**, in the **Delegate to** menu, select the identity to which you want to delegate the approval.
6. In the **Reason for your decision** field, enter a reason for the delegation.
7. Click **Save**.

#### ***To delegate approval of multiple attestation cases***

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases whose approval you want to delegate to another identity.
4. Click **⋮ (Actions) > Delegate approval**.
5. In the **Delegate approval**, in the **Delegate to** menu, select the identity to which you want to delegate the approval.
6. In the **Reason for your decision** field, enter a reason for the delegation.
7. Click **Save**.

#### **Related topics**

- [Withdrawing delegations from pending attestation case approvals](#) on page 64

## **Withdrawing delegations from pending attestation case approvals**

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

#### ***To withdraw an approval delegation***

1. In the menu bar, click **Attestation > Attestation history**.
2. On the **Attestation History** page, click **Details** next to the request whose approval delegation you want to withdraw.
3. In the **View Attestation Case Details** pane, click **Withdraw delegation**.
4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegation.
5. Click **Save**.

### ***To withdraw multiple delegations from approvals***

1. In the menu bar, click **Attestation > Attestation history**.
2. On the **Attestation History** page, in the list, select the check boxes next to the attestation cases whose approval delegations you want to withdraw.
3. Click **⋮ (Actions) > Withdraw delegation**.
4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegations.
5. Click **Save**.

### **Related topics**

- [Delegating approvals of pending attestation cases to other identities](#) on page 63

## **Rejecting approval of attestation cases**

If you have been added to an attestation case as an additional approver the approval of the attestation case was passed to you, you can reject the approval and return the attestation case to the original approver.

### ***To reject an approval***

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, click **Details** next to the attestation case that you do not want to make an approval decision about.
4. In the **View Attestation Case Details** pane, click **Reject approval**.
5. In the **Reject Approval**, in the **Reason for your decision** pane, enter a reason for the rejecting.
6. Click **Save**.

### ***To reject approval of multiple attestation cases***

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, perform one of the following actions:
  - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.

- To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases that you do not want to make an approval decision about.
  4. Click ⋮ (**Actions**) > **Reject approval**.
  5. In the **Reject Approval**, in the **Reason for your decision** pane, enter a reason for the rejecting.
  6. Click **Save**.

## Displaying attestation history

You can obtain an overview of all the attestation cases relevant to you or identities that report to you, by displaying the attestation history.

### *To display the attestation history*

1. In the menu bar, click **Attestation** > **Attestation history**.  
This opens the **Attestation History** page.
2. Perform one of the following actions:
  - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.
  - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Attestation policy**.
3. (Optional) To control which attestation cases are displayed, click ▼ (**Filter**) (see [Filtering](#) on page 16). For example, this allows you to show just pending attestation cases (no approval decision yet made).
4. (Optional) To display details of an attestation case, click **Details** next to the attestation case whose details you want to display.

### Related topics

- [Withdrawing delegations from pending attestation case approvals](#) on page 64

## Attestation – Administration

You can define attestation policies for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom. Once attestation is started, attestation cases are created that contain all the necessary information about the

attestation objects and the attester. The attester checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

### Detailed information about this topic

- [Attestation policies](#) on page 67
- [Starting attestation](#) on page 76
- [Attestation runs](#) on page 77
- [Attestation by peer group analysis](#) on page 79

## Attestation policies

You can define attestation policies for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom.


### Detailed information about this topic

- [Displaying attestation policies](#) on page 67
- [Setting up attestation policies](#) on page 68
- [Editing attestation policies](#) on page 71
- [Copying attestation policies](#) on page 73
- [Deleting attestation policies](#) on page 76
- [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 100

## Displaying attestation policies

You can display enabled and disabled attestation policies.

### *To display attestation policies*

1. In the menu bar, click **Attestation > Attestation Policies**.  
This opens the **Attestation Policies** page.
2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click  next to the filter (**Clear filter**).


### Related topics

- [Displaying attestation policies details](#) on page 68

## Displaying attestation policies details

To obtain an overview of an attestation policy, you can display its main data.


### *To show the details of an attestation policy*

1. In the menu bar, click **Attestation > Attestation Policies**.
2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click  next to the filter (**Clear filter**).
3. Next to the attestation policy whose details you want to show, click **Edit**.  
This opens the **Attestation Policy Settings** pane.
4. (Optional) To display the objects that fulfill the conditions, perform one of the following actions:
  - Objects that fulfill one condition: Under **Objects To Be Attested by This Attestation Policy**, click the number link next to the condition.
  - Objects that fulfill all conditions: Next to **Objects To Be Attested by This Attestation Policy**, click the number link.

## Displaying attestation policy reports

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

### *To display an attestation policy's report*

1. In the menu bar, click **Attestation > Attestation Policies**.
2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click  next to the filter (**Clear filter**).
3. On the **Attestation Policies** page, click  (**Actions**) > **Download report** next to the attestation policy whose report you want to display.  
Once the report is completely downloaded, you can open it.

### Related topics

- [Displaying attestation run reports](#) on page 79

## Setting up attestation policies

To fulfill new regulation requirements, you can create new attestation policies.

### To create a new attestation policy

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

**Table 7: Attestation policy main data**

Property	Description
Disabled	Specify whether the attestation policy is disabled or not. Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Completed attestation cases can be deleted once the attestation policy is disabled.
Attestation policy	Enter a name for the attestation policy.
Description	Enter a description of the attestation policy.
Attestation procedure	Select which objects to attest with this attestation policy. <b>NOTE:</b> The selection of the attestation procedure is crucial. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The available options are modified to match the attestation procedure.
Approval policies	Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.
Attestors	Click <b>Assign/Change</b> and then select the identities that can make approval decisions about attestation cases. <b>NOTE:</b> This field is only shown if you have selected an attestation policy in the <b>Attestation policy</b> menu that demands attestation by an approver (for example, <b>Attestation by selected approvers</b> ).
Calculation schedule	Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.
Time required (days)	Specify how many days attestors have to make an approval decision about the attestation cases governed by this policy. If you do not want to specify a time, enter <b>0</b> .
Owner	Select the identity that is responsible for this attestation policy. This identity can view and edit the attestation policy.
Risk index	Use the slider to define the attestation policy's risk index. This

Property	Description
	value specifies the risk for the company if attestation for this attestation policy is denied.
Compliance frameworks	Click <b>Assign/Change</b> and add a compliance framework to use. Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements. For example, internal requirements or auditing requirements.
Close obsolete tasks automatically	Specify whether attestation cases pending for this attestation policy are automatically closed if new attestation cases are created (for example, when there is a new attestation run of this attestation policy).  If an attestation run with this attestation policy is started and the option is set, new attestation cases are created according to the condition. All pending, obsolete attestation cases for newly determined attestation objects of this attestation policy are stopped. Attestation cases for attestation objects that are not recalculated, remain intact.
Approval by multi-factor authentication	Specify whether approvals about attestation cases governed by this attestation policy require multifactor authentication (for example Starling 2FA).

- To specify which objects to attest, under **Objects To Be Attested by This Attestation Policy**, click **Add condition**.
- In the **Condition type** menu, click the condition type to use (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 100).  
**NOTE:** The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.
- (Optional) Depending on which condition type you have selected, you can filter the selection of objects to attest (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 100).
- (Optional) Create more conditions if required. To do this, click **Add another condition**.
- (Optional) If you have specified more than one condition, you must specify whether one or all of the conditions must be fulfilled by enabling the appropriate option:
  - All conditions must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects fulfilling all of the conditions. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.

- **At least one condition must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects that fulfill at least one of the conditions. Use of this option generates a superset of all the individual conditions of the selected objects.

9. Click **Create**.

## Related topics

- [Appendix: Attestation conditions and approval policies from attestation procedures on page 100](#)

# Editing attestation policies

For example, you can modify attestation policies to include more conditions.

## To edit an attestation policy

1. In the menu bar, click **Attestation > Attestation Policies**.
2. On the **Attestation Policies** page, next to the attestation policy you want to edit, click **Edit**.

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

**NOTE:** The system contains default attestation policies. These policies can only be edited to a limited degree. If you want to make changes to a default attestation policy, create a copy and edit the copy (see [Copying attestation policies](#) on page 73).


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

**Table 8: Attestation policy main data**

Property	Description
Disabled	Specify whether the attestation policy is disabled or not. Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Completed attestation cases can be deleted once the attestation policy is disabled.
Attestation policy	Enter a name for the attestation policy.
Description	Enter a description of the attestation policy.
Attestation procedure	Select which objects to attest with this attestation policy. <b>NOTE:</b> The selection of the attestation procedure is crucial. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The

Property	Description
	available options are modified to match the attestation procedure.
Approval policies	Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.
Attestors	<p>Click <b>Assign/Change</b> and then select the identities that can make approval decisions about attestation cases.</p> <p><b>NOTE:</b> This field is only shown if you have selected an attestation policy in the <b>Attestation policy</b> menu that demands attestation by an approver (for example, <b>Attestation by selected approvers</b>).</p>
Calculation schedule	Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.
Time required (days)	Specify how many days attestors have to make an approval decision about the attestation cases governed by this policy. If you do not want to specify a time, enter <b>0</b> .
Owner	Select the identity that is responsible for this attestation policy. This identity can view and edit the attestation policy.
Risk index	Use the slider to define the attestation policy's risk index. This value specifies the risk for the company if attestation for this attestation policy is denied.
Compliance frameworks	<p>Click <b>Assign/Change</b> and add a compliance framework to use.</p> <p>Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements. For example, internal requirements or auditing requirements.</p>
Close obsolete tasks automatically	<p>Specify whether attestation cases pending for this attestation policy are automatically closed if new attestation cases are created (for example, when there is a new attestation run of this attestation policy).</p> <p>If an attestation run with this attestation policy is started and the option is set, new attestation cases are created according to the condition. All pending, obsolete attestation cases for newly determined attestation objects of this attestation policy are stopped. Attestation cases for attestation objects that are not recalculated, remain intact.</p>
Approval by	Specify whether approvals about attestation cases governed by

Property	Description
multi-factor authentication	this attestation policy require multifactor authentication (for example Starling 2FA).

4. To specify which objects to attest, perform one of the following actions:
    - To add a new condition, under **Objects To Be Attested by This Attestation Policy** click **Add another condition**.
    - To edit an existing condition, under **Objects To Be Attested by This Attestation Policy**, click the condition.
    - To delete an existing condition, click  (**Delete condition**).
  5. In the **Condition type** menu, click the condition type to use (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 100).
- NOTE:** The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.
6. (Optional) Depending on which condition type you have selected, you can filter the selection of objects to attest (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 100).
  7. (Optional) Create or modify more conditions if required. To do this, click **Add another condition**.
  8. (Optional) If you have specified more than one condition, you must specify whether one or all of the conditions must be fulfilled by enabling the appropriate option:
    - **All conditions must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects fulfilling all of the conditions. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.
    - **At least one condition must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects that fulfill at least one of the conditions. Use of this option generates a superset of all the individual conditions of the selected objects.
  9. Click **Save**.

## Related topics

- [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 100

## Copying attestation policies

You can copy existing attestation policies and then edit them. For example, if you want to make changes to a default attestation policy, you can copy it, edit the copy, and then use it.

Copied attestation policies can be deleted again.

### To copy an attestation policy


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

To view disabled attestation policies, clear the **Activated attestation policies only** filter. To do this, click **✕** next to the filter (**Clear filter**).
3. In the **Copy Attestation Policy** pane, edit the attestation policy's main data.

**Table 9: Attestation policy main data**

Property	Description
Disabled	Specify whether the attestation policy is disabled or not. Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Completed attestation cases can be deleted once the attestation policy is disabled.
Attestation policy	Enter a name for the attestation policy.
Description	Enter a description of the attestation policy.
Attestation procedure	Select which objects to attest with this attestation policy. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-left: 10px;"><p><b>NOTE:</b> The selection of the attestation procedure is crucial. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The available options are modified to match the attestation procedure.</p></div>
Approval policies	Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.
Attestors	Click <b>Assign/Change</b> and then select the identities that can make approval decisions about attestation cases. <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-left: 10px;"><p><b>NOTE:</b> This field is only shown if you have selected an attestation policy in the <b>Attestation policy</b> menu that demands attestation by an approver (for example, <b>Attestation by selected approvers</b>).</p></div>
Calculation schedule	Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.
Time required (days)	Specify how many days attestors have to make an approval decision about the attestation cases governed by this policy. If you do not want to specify a time, enter <b>0</b> .

Property	Description
Owner	Select the identity that is responsible for this attestation policy. This identity can view and edit the attestation policy.
Risk index	Use the slider to define the attestation policy's risk index. This value specifies the risk for the company if attestation for this attestation policy is denied.
Compliance frameworks	Click <b>Assign/Change</b> and add a compliance framework to use. Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements. For example, internal requirements or auditing requirements.
Close obsolete tasks automatically	Specify whether attestation cases pending for this attestation policy are automatically closed if new attestation cases are created (for example, when there is a new attestation run of this attestation policy).  If an attestation run with this attestation policy is started and the option is set, new attestation cases are created according to the condition. All pending, obsolete attestation cases for newly determined attestation objects of this attestation policy are stopped. Attestation cases for attestation objects that are not recalculated, remain intact.
Approval by multi-factor authentication	Specify whether approvals about attestation cases governed by this attestation policy require multifactor authentication (for example Starling 2FA).

4. To specify which objects to attest, perform one of the following actions:
  - To add a new condition, under **Objects To Be Attested by This Attestation Policy** click **Add another condition**.
  - To edit an existing condition, under **Objects To Be Attested by This Attestation Policy**, click the condition.
  - To delete an existing condition, click  (**Delete condition**).
5. In the **Condition type** menu, click the condition type to use (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 100).
 

**NOTE:** The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.
6. (Optional) Depending on which condition type you have selected, you can filter the selection of objects to attest (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 100).

7. (Optional) Create or modify more conditions if required. To do this, click **Add another condition**.
8. (Optional) If you have specified more than one condition, you must specify whether one or all of the conditions must be fulfilled by enabling the appropriate option:
  - **All conditions must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects fulfilling all of the conditions. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.
  - **At least one condition must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects that fulfill at least one of the conditions. Use of this option generates a superset of all the individual conditions of the selected objects.
9. Click **Create**.

## Related topics



- [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 100

## Deleting attestation policies

You can delete attestation policies that are not used anymore.

**NOTE:** You can only delete attestation policies if no attestation cases are associated with it anymore.

### *To delete an attestation policy*

1. In the menu bar, click **Attestation > Attestation Policies**.
2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click  next to the filter (**Clear filter**).
3. On the **Manage Attestation Policies** page, click  (**Actions**) > **Delete** next to the attestation policy you want to delete.
4. In the **Delete attestation policy** dialog, confirm the prompt with **OK**.

## Starting attestation

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

### ***To start attestation using a scheduled task***

1. In the menu bar, click **Attestation > Attestation Policies**.
2. On the **Attestation Policies** page, next to the attestation you want to start, click **(Actions) > Edit**.  
| **TIP:** To display disabled attestation policies, enable the **Show disabled policies**.
3. In the **Edit attestation policy** pane, deselect the **Disabled** box.
4. In the **Calculation schedule** menu, specify how often an attestation run with this attestation policy is started.

Each attestation run creates a new attestation case respectively.

### ***To start attestation for selected objects***

1. In the menu bar, click **Attestation > Attestation Policies**.
2. On the **Attestation Policies** page, next to the attestation policy that you want to start, click **(Actions) > Start attestation**.
3. In the **Start attestation** pane, perform one of the following actions:
  - To start attesting an object, click **Start attestation** next to the object.
  - To start attesting several object, select the check box in front of each object and click **Start attestation for selected**.
  - To start attesting all objects, click **Start attestation for all**.

### **Related topics**

- [Editing attestation policies](#) on page 71

## **Attestation runs**

Once attestation has started, a corresponding attestation run is added that, in turn, creates an attestation case. Attestation runs show you the attestation prediction and give you an overview of pending attestation cases.

### **Detailed information about this topic**

- [Displaying attestation policy runs](#) on page 77
- [Sending reminders about attestation runs](#) on page 57
- [Extending attestation runs](#) on page 79

## **Displaying attestation policy runs**

You can the display attestation runs of attestation policies.

### ***To display attestation policy runs***

1. In the menu bar, click **Attestation > Attestation runs**.  
This opens the **Attestation Policy Runs** page
2. (Optional) To display more details of an attestation run (current date, details about attestation, attestation prediction, and attestors), click **Details** next to the attestation run, then the information is displayed in the details pane.

### **Related topics**

- [Sending reminders about attestation runs](#) on page 57

## **Displaying attestation cases of application runs**

You can view all attestation cases created in an attestation run. In addition, you can approve or reject pending attestation cases.

### ***To display attestation cases of an attestation run***

1. In the menu bar, click **Attestation > Attestation runs**.
2. On the **Attestation Runs** page, click **Details** next to the attestation run with the attestation cases you want to display.
3. In the **View Attestation Run Details** pane, click the **Attestation cases** tab.
4. (Optional) To further limit the attestation cases to be displayed, click ▼ (**Filter**) on the **Attestation cases** tab.
5. (Optional) To approve or deny an attestation case, perform the following actions in the **Attestation cases** tab:
  - a. Select the check box in front of the attestation case that you want to approve or deny.
  - b. Click **Approve** or **Deny**.
  - c. In the **Approve Attestation Case/Deny Attestation Case** pane, enter a reason for your approval decision in the **Reason for decision** field.
  - d. Click **Save**.
6. (Optional) To view more details of an attestation process, click **Details** next to the attestation process and refer to the **View Attestation Process Details** pane for the relevant information.

### **Related topics**

- [Displaying pending attestation cases](#) on page 58
- [Granting or denying attestation cases](#) on page 58

## Displaying attestation run reports

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

### *To display an attestation run's report*

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

### Related topics

- [Displaying attestation policy reports](#) on page 68

## Extending attestation runs

You can extend attestation runs.

### *To extend an attestation run*

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

### Related topics

- [Sending reminders about attestation runs](#) on page 57

## Attestation by peer group analysis

Using peer group analysis, approval for attestation cases can be granted or denied automatically. For example, a peer group might be all identities in the same department. Peer group analysis assumes that these identities require the same system entitlements. For example, if the majority of identities belonging to a department have a system

entitlement, assignment to another identity in the department can be approved automatically. This helps to accelerate approval processes.

Peer group analysis can be used during attestation of the following memberships:

- Assignments of system entitlements to user accounts
- Secondary memberships in business roles

All identities that have the same manager or that belong to the same primary or secondary division as the identity linked to the attestation object (= identity to be attested) are grouped together as a peer group.

For more information about peer group analysis, see the *One Identity Manager Attestation Administration Guide*.

## Related topics

- [Appendix: Attestation conditions and approval policies from attestation procedures on page 100](#)

# Responsibilities

In One Identity Manager, identities have responsibilities for various objects. In the Web Portal, you can perform a number of actions on these responsibilities and obtain information about them.

## Detailed information about this topic

- [My responsibilities](#) on page 81
- [Delegating tasks](#) on page 85
- [Ownerships](#) on page 87

## My responsibilities

You can manage objects that you are responsible for within your company. Possible objects are:

- Identities

## Detailed information about this topic

- [My identities](#) on page 81

## My identities

You can carry out various actions on the identities that you manage and obtain information about them.

## Detailed information about this topic

- [Displaying my identities](#) on page 82
- [Deactivating my identities](#) on page 82

- [Reactivating my identities](#) on page 83

## Displaying my identities

You can see all the identities for which you are responsible.

### *To display identities*

1. In the menu bar, click **Home**.
2. On the home page, click **Show** in the **My Direct Reports** tile.  
This opens the **Identities** page and displays all the identities that report directly to you.
3. (Optional) To display details of an identity, click it in the list.  
**TIP:** To create a report about an identity, click **Download report**.

## Deactivating my identities

You can deactivate identities permanently such as when an employee leaves a company. This may be necessary to strip these identities of their permissions in the connected target system and from their company resources.

Effects of permanent deactivating an identity are:

- The identity cannot be assigned to identities as a manager.
- The identity cannot be assigned to roles as a supervisor.
- The identity cannot be assigned to attestation policies as an owner.
- The identity's user accounts are locked or deleted and then removed from group memberships.

### *To deactivate an identity*

1. In the menu bar, click **Home**.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity you want to deactivate.
4. In the details pane, expand the **Organizational Information** section.
5. In the **Organizational Information** section, select the **Permanently deactivated** check box.
6. Click **Save**.

## Reactivating my identities

You can activate permanently deactivated identities if they have not been deactivated by certification.

### *To reactivate an identity*

1. In the menu bar, click **Home**.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity you want to activate.
4. In the details pane, expand the **Organizational Information** section.
5. In the **Organizational Information** pane, clear the **Permanently deactivated** check box.
6. Click **Save**.

## My identities' attestations

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use the One Identity Manager attestation functionality to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom. Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in an attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

### Detailed information about this topic

- [Displaying my identities' attestation cases](#) on page 84
- [Approving and denying attestation cases of my identities](#) on page 84

## Displaying my identities' attestation cases

You can see attestation cases that involve identities for which you are responsible. In addition, you can obtain more information about the attestation cases.

1. In the menu bar, click **Home**.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. In the details pane, click the **Attestation** tab.  
This displays all the identity's attestation cases.
5. (Optional) To display more details of an attestation case, click **Details** next to the attestation case.

### Related topics

- [Attestation](#) on page 56
- [Displaying pending attestation cases](#) on page 58

## Approving and denying attestation cases of my identities

You can grant or deny approval to attestation cases of identities for which you are responsible.

### *To approve an attestation case*

1. In the menu bar, click **Home**.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity whose attestation cases you want decide.
4. In the details pane, click the **Attestation** tab.
5. On the **Attestation** tab, perform the following actions:
  - To approve an attestation case, in the list, select the check box next to the attestation case and click **Approve** below the list.
  - To deny an attestation case, in the list, select the check box next to the attestation case and click **Deny** below the list.
6. (Optional) In the **Approve/Deny** pane, perform one of the following actions:
  - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
  - b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

**TIP:** By giving reasons, your approvals are more transparent and support the

| audit trail.

7. Click **Save**.

### Related topics

- [Attestation](#) on page 56
- [Granting or denying attestation cases](#) on page 58

## Delegating tasks

You can temporarily delegate role memberships and responsibilities (and associated entitlements and duties) to other identities.

For example, if you go on vacation, you can hand over responsibility for a department and the associated tasks to a deputy.

Role memberships and responsibilities can also be delegated to you.

| **NOTE:** In the Web Portal, a delegation is treated like a request.

### Detailed information about this topic

- [Displaying delegations](#) on page 85
- [Creating delegations](#) on page 85
- [Canceling delegations](#) on page 86
- [Deleting delegations](#) on page 87

## Displaying delegations

You can see delegations created by you or by others for you.

### *To display delegations*

1. In the menu bar, click **Requests** > **Request History**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, select the **My delegations** check box.
4. (Optional) To display more details about a delegation, click **Details** next to the delegation whose details you want to show.

## Creating delegations

You can delegate role memberships and responsibilities to other identities.

**NOTE:** You cannot edit a delegation afterward. If you want to make a change to the delegation, delete the it (see [Deleting delegations](#) on page 87) and create a new delegation.

### ***To create a delegation***

1. In the menu bar, click **Responsibilities > Delegation**.
2. On the **Create Delegation** page, in the **Delegation recipient** field, select the identity to which you want to delegate.
3. Click **Next**.
4. In the **Select the type of delegation** step, perform one of the following actions:
  - To delegate all memberships and responsibilities (grouped by topic), set **Delegate all memberships and responsibilities**.
  - To delegate individual memberships and responsibilities, set **Select individual memberships and responsibilities to delegate**.
5. Click **Next**.
6. In the **Select the role membership/responsibility you want to delegate** step, in the list, select the check boxes in front of the role memberships/responsibilities you want to delegate.
7. Click **Next**.
8. In the **Add additional information** set, configure the following settings:
  - **Valid from:** Specify from when the role/responsibility will be delegated.
  - **Valid until:** Specify until when the role/responsibility will be delegated.
  - **Notify me if the recipient of the delegation makes a decision:** (Optional) Select the check box if you want to be notified when the recipient makes an approval decision about a delegated role/responsibility.
  - **The recipient can delegate this role:** (Optional) Select the check box to specify that the recipient can delegate their delegated role/responsibility on to another identity.
  - **Reason:** (Optional) In the dialog, enter a reason for the delegation.
  - **Priority:** (Optional) In the menu, select a priority for the delegation.
9. Click **Save**.

## **Canceling delegations**

You can cancel delegations that you have already set up.

**NOTE:** You can only cancel delegations as long they have the **Request** or **Approved** status. You can delete delegations with the **Assigned** status (see [Deleting delegations](#) on page 87).

### ***To cancel a delegation***

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, select the **My delegations** check box.
4. Next to the delegation you want to cancel, click **Details**.
5. In the **View Request Details** pane, click **Cancel request**.
6. (Optional) In the **Cancel request** pane, in the **Reason for your decision** field, enter a reason for the cancellation.
7. Click **Save**.

## **Deleting delegations**

You can delete delegations that you created. That is, responsibilities that you have delegated to others become your responsibility again.

**NOTE:** You can only delete delegations as long as they have the **Assigned** status. You can cancel delegations that have the **Request** or **Approved** status (see [Canceling delegations](#) on page 86).

### ***To delete a delegation***

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, select the **My delegations** check box.
4. Next to the delegation you want to delete, click **Details**.
5. In the **View Request Details** pane, click **Unsubscribe product**.
6. In the **Unsubscribe Product** pane, perform the following actions:
  - a. In the **Unsubscribed as from** field, specify the date on which to delete the delegation. If you leave this field empty, the delegation is deleted once you have clicked **Saved**.
  - b. In the **Reason for your decision** field, enter a reason for your approval decision.
  - c. In the **Additional comments about your decision** field, enter extra information.
  - d. Click **Save**.

## **Ownerships**

You can assign business objects to owners or assume ownership of them.

## Detailed information about this topic

- [Assigning product owners to system entitlements](#) on page 88

# Assigning product owners to system entitlements

You can assign a product owner to a system entitlements that do not have one or assume ownership of them yourself.

### *To assign a product owner to a system entitlement*

1. In the menu bar, click **Responsibilities > Assign Ownership**.
2. On the **Assign an Owner for a System Entitlement** page, in the **System entitlement** menu, select the system entitlement that you want to assign a product owner to.
3. Click **Next**.
4. In the second step, perform one of the following actions:
  - To assume ownership yourself, click **I want to take ownership of this system entitlement**.
  - To specify another identity as the product owner, click **Select another owner** or **Select from the suggested possible owners** and select the identity in the **Designated owner** menu.
5. Click **Next**.

In the context of an attestation, the selected product owner can confirm that this assignment is correct (see [Pending attestations](#) on page 57).

## Setting up and configuring request functions

In order to request products in the Web Portal, the Web Portal must be set up accordingly. Application roles help you to define who can take over administrative tasks in the Web Portal.

### Structure and workflow of requests

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

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

Requests follow a defined approval process that determines whether a product may be assigned or not. Authorized identities have the option to approve requests and cancellations. You determine which approval process to use by assigning approval policies to shops or shelves (see [Editing shop details](#) on page 92 and [Editing shelf details](#) on page 95).

### Detailed information about this topic

- [Managing shops](#) on page 89

## Managing shops

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

A shop can contain several shelves (see [Managing shop shelves](#) on page 93). Products are assigned to these shelves and can then be requested (see [Managing requestable products in shops](#) on page 97).

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

You can also decide who is able to request products from shops (see [Managing access to requestable system entitlements in shops](#) on page 96).

### Detailed information about this topic

- [Displaying shops](#) on page 90
- [Creating shops](#) on page 90
- [Editing shops](#) on page 91
- [Deleting shops](#) on page 92
- [Managing shop shelves](#) on page 93
- [Managing access to requestable system entitlements in shops](#) on page 96
- [Managing requestable products in shops](#) on page 97

## Displaying shops

You can display any of the shops and their details.

### *To display shops*

1. In the menu bar click **Setup > Shops**.  
This opens the **Shops** page.
2. (Optional) To display details of a shop, in the list, click on the shop.
3. (Optional) You can perform the following actions:
  - You can see the shop's shelves (see [Displaying shop shelves](#) on page 93).
  - You can display who can request products from the shop (see [Displaying shop members](#) on page 96).

## Creating shops

To set up your own shop solution, you can create shops. You can then customize these shops as you wish (see [Editing shops](#) on page 91).

### *To create a shop*

1. In the menu bar click **Setup > Shops**.
2. On the Shops page click **Create Shop**.
3. In the **Create Shop** pane, enter the main data for the new shop.

**Table 10: Shop main data**

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

4. Click **Create**.
5. (Optional) Create shelves for the shop (see [Creating shelves for shops](#) on page 93). In the shelves, you can specify which products can be requested from the shop (see [Adding products to shelves](#) on page 98).
6. (Optional) To specify who can request products from the shop, add members to the shop (see [Adding members to shops](#) on page 97).

## Editing shops

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

- Edit shop details (see [Editing shop details](#) on page 92)
- Manage shop shelves (see [Managing shop shelves](#) on page 93)
- Specify who can request products from shops (see [Managing access to requestable system entitlements in shops](#) on page 96)
- Specify which products can be requested from shops (see [Managing requestable products in shops](#) on page 97)

# Editing shop details

You can edit details of existing shops.

## *To edit details of a shop*

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

**Table 11: Shop main data**

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

4. Click **Save**.

# Deleting shops

You can delete shops.

**NOTE:** Before you can delete a shop, you must delete all shelves from the shop (see [Deleting shelves from shops](#) on page 96) and remove all members from the shop (see [Removing members from shops](#) on page 97).

### ***To delete a shop***

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

## **Managing shop shelves**

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

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

### **Detailed information about this topic**

- [Displaying shop shelves](#) on page 93
- [Creating shelves for shops](#) on page 93
- [Editing shop shelves](#) on page 94
- [Editing shelf details](#) on page 95
- [Deleting shelves from shops](#) on page 96

## **Displaying shop shelves**

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

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

### ***To display the shelves in a store***

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, in the list, click the shop whose shelves you want to display.
3. In the **Edit Shop** pane, click the **Shelves** tab.
4. (Optional) To display details of a shelf, click it in the list.
5. (Optional) You can display the products that can be requested over this shelf (see [Displaying requestable products](#) on page 98).

## **Creating shelves for shops**

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

### To create a shelf for shop

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

**Table 12: Shelves main data**

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

6. Click **Create**.
7. (Optional) To specify which products can be requested from the shelf, add the corresponding products to the shelf (see [Adding products to shelves](#) on page 98).

## Editing shop shelves

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

- Edit shelf details (see [Editing shop details](#) on page 92)
- Specify which products can be requested from shops (see [Managing requestable products in shops](#) on page 97)

## Editing shelf details

You can edit details of existing shelves.

### *To edit details of a shelf*

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

**Table 13: Shelves main data**

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

6. Click **Save**.

## Related topics

- [Managing requestable products in shops](#) on page 97

## Deleting shelves from shops

You can delete shops.

**NOTE:** Before you can delete a shelf, you must remove all the products from it (see [Removing products from shelves](#) on page 99).

### *To delete a shelf from a shop*

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

## Managing access to requestable system entitlements in shops

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

### Detailed information about this topic

- [Displaying shop members](#) on page 96
- [Adding members to shops](#) on page 97
- [Removing members from shops](#) on page 97

## Displaying shop members

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

### *To display members of a shop*

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, in the list, click the shop whose members you want to display.

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

## Adding members to shops

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

### *To add a member to a shop*

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, in the list, click the Shop you want to add a member to.
3. In the **Edit Shop** pane, click the **Access** tab.
4. On the **Access** tab, click **Add members**.
5. In the **Add members** dialog, select the check box in front of the identity that you want to add to the shop as a member.
6. Click **Apply**.

## Removing members from shops

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

### *To remove a member from a shop*

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, in the list, click the Shop from which you want to remove a member.
3. In the **Edit Shop** pane, click the **Access** tab.
4. On the **Access** tab, in the list, select the check box next to the identity that you want to remove as a member.
5. Click **Remove**.

## Managing requestable products in shops

You can decide which products can be requested from shops. Once products have been allocated to shelves in a shop (see [Adding products to shelves](#) on page 98) and labeled as requestable, they can be requested in the Web Portal by members of the shop.

## Detailed information about this topic

- [Displaying requestable products](#) on page 98
- [Adding products to shelves](#) on page 98
- [Removing products from shelves](#) on page 99

## Displaying requestable products

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

### *To display a shelf's requestable products*

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, click the shop in the list whose requestable products you want to display.
3. In the **Edit Shop** pane, click the **Shelves** tab.
4. On the **Shelves** tab, in the list, click the shelf with the requestable products you want to display.
5. In the **Edit shelf** pane, click the **Products** tab.

## Adding products to shelves

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

### *To add a product to a shelf*

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, in the list, click the shop that you want request the system entitlement from later.
3. In the **Edit Shop** pane, click the **Shelves** tab.
4. On the **Shelves** tab, in the list, click the shelf to add the system entitlement to.
5. In the **Edit shelf** pane, click the **Products** tab.
6. On the **Products** tab, click **Add products**.
7. In the **Add Products** dialog, select the type of product you want to add from the menu.
8. Select the check box in front of the product that you want to add to the shelf.
9. Click **Apply**.

## Removing products from shelves

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

### *To remove a product from a shelf*

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, in the list, click the shop from whose shelf you want to remove the system entitlement.
3. In the **Edit Shop** pane, click the **Shelves** tab.
4. On the **Shelves** tab, in the list, click the shelf to remove the product from.
5. In the **Edit shelf** pane, click the **Products** tab.
6. On the **Products** tab, select the check box in front of the product that you want to remove from the shelf.
7. Click **Remove**.

## Appendix: Attestation conditions and approval policies from attestation procedures



When attestation policies are created or edited (see [Setting up attestation policies](#) on page 68 or [Editing attestation policies](#) on page 71), you specify attestation conditions and approval policies:



- Attestation procedures specify which objects to attest. They define the properties of the attestation objects to attest.
- There are different attestation conditions for each attestation procedure that you use to specify which objects to attest.
- Attestors for each attestation case are determined by approval policies.

In the following chapter, you will find more information about the various attestation procedures and associated approval policies and attestation conditions.

### Attesting primary departments





Primary identity memberships in departments are attested using the **Primary department attestation** attestation procedure.

Condition	Description
All departments	Attests primary memberships in all departments.
Specific departments	Select the departments with primary memberships to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific child departments	Select the departments with primary memberships to attest. In addition, primary memberships of all child departments under this

Condition	Description
	department are attested. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Departments with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests primary memberships in departments with a risk index in the chosen range.
Departments with matching name	Enter part of a name of departments with primary memberships to attest. All departments that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.





## Attesting primary business roles

Primary identity memberships in business roles are attested using the **Primary business role attestation** attestation procedure.

Condition	Description
All business roles	Attests primary memberships in all business roles.
Specific business roles	Select the business roles with primary memberships to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific child business roles	Select the business roles with primary memberships to attest. In addition, primary memberships of all child business roles under this business role are attested. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Business roles with specific role classes	Select the role classes. Attests primary membership in business roles with this role class.
Business roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests primary memberships in business roles with a risk index in the chosen range.
Business roles with matching name	Enter part of a name of business roles with primary memberships to attest. All business roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.





# Attesting primary cost centers

Primary identity memberships in cost centers are attested using the **Primary cost center attestation** attestation procedure.

Condition	Description
All cost centers	Attests primary memberships in all cost centers.
Specific cost centers	Select the cost centers with primary memberships to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific child cost centers	Select the cost centers with primary memberships to attest. In addition, primary memberships of all child cost centers under this cost center are attested. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Cost centers with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests primary memberships in cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with primary memberships to attest. All cost centers that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

# Attesting primary locations





Primary identity memberships in locations are attested using the **Primary location attestation** attestation procedure.

Condition	Description
All locations	Attests primary memberships in all locations.
Specific locations	Select the locations with primary memberships to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific child locations	Select the locations with primary memberships to attest. In addition, primary memberships of all child locations under this location are attested. Use  and  to switch between hierarchical and list view. Multi-select is possible.

Condition	Description
	possible.
Locations with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests primary memberships in locations with a risk index in the chosen range.
Locations with matching name	Enter part of a name of locations with primary memberships to attest. All locations that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.





## Attesting secondary departments

Secondary identity memberships in departments are attested using the **Secondary department attestation** attestation procedure.

Condition	Description
All departments	Attests secondary memberships in all departments.
Specific departments	Select the departments with secondary memberships to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific child departments	Select the departments with secondary memberships to attest. In addition, secondary memberships of all child departments under this department are attested. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Departments with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests secondary memberships in departments with a risk index in the chosen range.
Departments with matching name	Enter part of a name of departments with secondary memberships to attest. All departments that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.





# Attesting secondary cost centers

Secondary identity memberships in cost centers are attested using the **Secondary cost center attestation** attestation procedure.

Condition	Description
All cost centers	Attests secondary memberships in all cost centers.
Specific cost centers	Select the cost centers with secondary memberships to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific child cost centers	Select the cost centers with secondary memberships to attest. In addition, secondary memberships of all child cost centers under this cost center are attested. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Cost centers with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests secondary memberships in cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with secondary memberships to attest. All cost centers that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

# Attesting secondary locations

Secondary identity memberships in locations are attested using the **Secondary location attestation** attestation procedure.

Condition	Description
All locations	Attests secondary memberships in all locations.
Specific locations	Select the locations with secondary memberships to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific child locations	Select the locations with secondary memberships to attest. In addition, secondary memberships of all child locations under this location are attested. Use  and  to switch between hierarchical and list view. Multi-select is possible.

Condition	Description
	possible.
Locations with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests secondary memberships in locations with a risk index in the chosen range.
Locations with matching name	Enter part of a name of locations with secondary memberships to attest. All locations that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting PAM asset groups

PAM asset groups are attested using the **PAM asset group attestation** attestation procedure.

Condition	Description
All PAM asset groups	Attests all PAM assets groups.
Specific PAM asset groups	Select the PAM asset groups to attest.
PAM asset groups on specific systems	Select the PAM appliances with PAM asset groups to attest.
PAM asset groups with matching name	Enter part of a name of PAM asset groups with access to attest. All PAM asset groups that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting PAM asset accounts

PAM asset accounts are attested using the **PAM asset account attestation** attestation procedure.

Condition	Description
All PAM asset accounts	Attests all PAM asset accounts.

Condition	Description
Specific PAN asset accounts	Select the PAM asset accounts to attest.
PAM asset accounts on specific systems	Select the PAM appliances with PAM asset accounts to attest.
PAM asset accounts with matching name	Enter part of a name of PAM asset accounts with access to attest. All PAM asset accounts that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting PAM assets

PAM assets are attested using the **PAM asset attestation** attestation procedure.

Condition	Description
All PAM assets	Attests all PAM assets.
Specific PAM assets	Select the PAM assets to attest.
PAM assets on specific systems	Select the PAM appliances with PAM asset to attest.
PAM assets with matching name	Enter part of a name of PAM assets with access to attest. All PAM assets that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting PAM user groups

PAM user groups are attested using the **PAM user group attestation** attestation procedure.

Condition	Description
All PAM user groups	Attests all PAM user groups.

Condition	Description
Specific PAM user groups	Select the PAM user groups to attest.
PAM user groups with matching name	Enter part of a name of PAM user groups with access to attest. All PAM user groups that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting PAM user accounts

PAM user accounts are attested using the **PAM user account attestation** attestation procedure.

Condition	Description
All PAM user accounts	Attests all PAM user accounts.
Specific permissions	Select the permissions. Attests PAM user accounts with these permissions.
Specific PAM user accounts	Select the PAM user accounts to attest.
PAM user accounts in specific user groups	Select the user groups. Attests PAM user accounts that belong to these user groups.
PAM user groups on specific systems	Select the PAM appliances with PAM user groups to attest.
PAM user accounts mapped to specific employees	Select the identities. Attests PAM user accounts that are assigned these identities.
PAM user accounts with matching name	Enter part of a name of PAM user accounts with access to attest. All PAM user accounts that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

# Attesting PAM account groups

PAM account groups are attested using the **PAM account group attestation** attestation procedure.

Condition	Description
All PAM account groups	Attests all PAM account groups.
Specific PAM account groups	Select the PAM account groups to attest.
PAM user accounts on specific systems PAM account groups on specific systems	Select the PAM appliances with PAM user accounts to attest. Select the PAM appliances with PAM account groups to attest.
PAM account groups with matching name	Enter part of a name of PAM account groups with access to attest. All PAM account groups that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

# Attesting PAM directory accounts

PAM directory accounts are attested using the **PAM directory account attestation** attestation procedure.

Condition	Description
All PAM directory accounts	Attests all PAM directory accounts.
Specific PAM directory accounts	Select the PAM directory accounts to attest.
PAM directory accounts on specific direct-	Select the directories. Attests directory accounts that are found in this directory.

Condition	Description
ories	
PAM directory accounts with matching name	Enter part of a name of PAM directory accounts with access to attest. All PAM directory accounts that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting PAM accesses

PAM access are attested using the **PAM access attestation** attestation procedure.



Condition	Description
All PAM accesses	Attests all PAM access.
Specific PAN asset accounts	Select the PAM asset accounts with access to attest.
Specific PAM assets	Select the PAM assets with access to attest.
Specific PAM user accounts	Select the PAM user accounts with access to attest.
Specific PAM directory accounts	Select the PAM directory accounts with access to attest.
Specific PAM directories	Select PAM directories. Attests access to these PAM directories.
Specific access type	Select access types. Attests access that uses one of these access types.
PAM user accounts mapped to specific employees	Select the identities. Attests access through PAM user accounts with these identities assigned to them.
PAM user accounts with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests access through PAM user accounts with a risk index in the chosen range.
PAM user	Enter part of a name of PAM user accounts with access to attest. All PAM

Condition	Description
accounts with matching name	user accounts that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting departments

Department properties are attested using the **Department attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All departments	Attests all departments.
Specific departments	Select the departments to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Departments with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests departments with a risk index in the chosen range.
Departments with matching name	Enter part of a name of departments with access to attest. All departments that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.



For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases.
Attestation of departments by manager	Department managers can make approval decisions through attestation cases.

## Application role attestation

Application role properties are attested using the **Application role attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All application roles	Attests all application roles.
Specific application roles	Select the application roles to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Application roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests application roles with a risk index in the chosen range.
Application roles with matching name	Enter part of a name of application roles with access to attest. All application roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.



For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases.

## Business role attestation

Business role properties are attested using the **Business role attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All business roles	Attests all business roles.
Specific business roles	Select the business roles to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Business roles with specific role classes	Select the role classes. Attests business roles with these role classes.
Business roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests business roles with a risk index in the chosen range.

Condition	Description
Business roles with matching name	Enter part of a name of business roles with access to attest. All business roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.



For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases.
Attestation of business roles by manager	Business role managers can make approval decisions through attestation cases.
Certification of business roles	Business role managers can make approval decisions through attestation cases.

## Attesting system roles

Cost center properties are attested using the **Cost center attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All cost centers	Attests all cost centers.
Specific cost centers	Select the cost centers to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Cost centers with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with access to attest. All cost centers that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.



For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases.
Attestation of cost centers by manager	Cost center managers can make approval decisions through attestation cases.

## Attesting locations

Location properties are attested using the **Location attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All locations	Attests all locations.
Specific locations	Select the locations to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Locations with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests locations with a risk index in the chosen range.
Locations with matching name	Enter part of a name of locations with access to attest. All locations that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.



For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases.
Attestation of locations by manager	Location managers can make approval decisions through attestation cases.

# Attesting system roles

System role properties are attested using the **System role attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All system roles	Attests all system roles.
Specific system roles	Select the system roles to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
System roles by applications	Select the applications (Application Governance). Attests system roles that are assigned to these applications.
System roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests system roles with a risk index in the chosen range.
System roles with matching name	Enter part of a name of system roles with access to attest. All system roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases.
Attestation of system roles by manager	System role managers can make approval decisions through attestation cases.

# Attesting memberships in system entitlements

User account memberships in system entitlements are attested using the **System entitlements membership attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All system entitlements	Attests memberships in all system entitlements.
Specific employees	Select the identities. Attests this identity's memberships (or their associated user accounts) in system entitlements.
Specific employees with subidentities.	Select the identities. Attests this identity's memberships (or their associated user accounts) in system entitlements. In addition, it attests sub identities' memberships (or their associated user accounts) that the select identities are assigned to.
Specific system entitlements	Select the system entitlements. Attests memberships in these system entitlements.
Membership by attestation state	<p>Select an attestation status Attests memberships in system entitlements that match this attestation status.</p> <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests memberships that have been denied.</li> <li>• <b>All Memberships:</b> Attests all memberships.</li> <li>• <b>New memberships:</b> Attests memberships that have never been attested.</li> </ul>
New or not attested for x days	Specify a number of days. Attests memberships in system entitlements that have not been attested for the defined number of days.
No dynamic groups from Active Roles	Attests memberships in all system entitlements. Dynamic groups are ignored in the process.
System entitlements with specific owners	Select the identities. Attests memberships in system entitlements that are managed by these identities.
System entitlements in a target system container	Select the target system containers. Attests memberships in system entitlements found in these target system containers.
System entitlements in target systems	Select the target systems. Attests memberships in system entitlements assigned to these target systems.
System entitlements with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests memberships in system entitlements with a risk index in the chosen range.

Condition	Description
System entitlements with owners in departments	Select the departments. Attests memberships in system entitlements that are managed by the identities in these departments.
System entitlements with any owner	Attests user account memberships in system entitlements that only have one owner.
System entitlements with matching name	Enter part of a name of system entitlements with user account memberships to attest. All system entitlements that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
System entitlements by applications	Select the applications. Attests user account memberships in system entitlements that are assigned to these applications.
System entitlements by assignment origin	<p>Select how user account memberships in system entitlements must be assigned to enable attestation:</p> <ul style="list-style-type: none"> <li>• <b>Directly assigned:</b> Attests memberships that were assigned directly.</li> <li>• <b>By request:</b> Attests memberships in system entitlements that were requested.</li> <li>• <b>By dynamic roles:</b> Attests memberships in system entitlements that were assigned through dynamic roles.</li> <li>• <b>Through roles:</b> Attests memberships in system entitlements that were assigned through roles.</li> <li>• <b>Through system roles:</b> Attests memberships in system entitlements that were assigned through system roles.</li> </ul>

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases.
Attestation by selected approvers with automatic removal of assignments	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.
Attestation by entitlement owner with automatic removal of assignments	Product owners of system entitlements can be approved through attestation cases. Memberships are deleted if attestation is denied and the configuration fits.



Approval policies	Description
Attestation by employee manager and product owner (with peer group analysis)	<p>The following identities can be approved through attestation cases:</p> <ul style="list-style-type: none"> <li>• Identity managers who are assigned the system entitlements</li> <li>• Product owners of system entitlements after a peer group analysis (see <a href="#">Attestation by peer group analysis</a> on page 79)</li> </ul>
Attestation of group memberships by product owner with automatic removal of memberships	Product owners of system entitlements can be approved through attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

## Attesting memberships in application roles

Memberships in application roles are attested using the **Application role membership attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All roles	Attests memberships in all applications roles.
Application roles with matching name	<p>Enter part of a name of application roles with primary memberships to attest. All application roles that have this pattern in their name are included.</p> <p>Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.</p>
Attesting by attestation status	<p>Select an attestation status Attests memberships in application roles that match this attestation status.</p> <p>You can select the follow status:</p> <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests memberships that have been denied.</li> <li>• <b>All Memberships:</b> Attests all memberships.</li> <li>• <b>New memberships:</b> Attests memberships that have never been attested.</li> </ul>
Specific employees	Select the identities. Attests identity memberships in application roles.
Specific	Select the identities. Attests identity memberships in application roles.

Condition	Description
employees with subidentities.	In addition, this identity's subidentities memberships in application roles are attested.
Specific roles	<p>Select the application roles. Attests memberships in these application roles.</p> <p>Use  and  to switch between hierarchical and list view. Multi-select is possible.</p>
New or not attested for x days	Specify a number of days. Attests memberships in application roles that have not been attested for the defined number of days.
Roles by assignment type	<p>Select how memberships in application roles must be assigned to enable attestation:</p> <ul style="list-style-type: none"> <li>• <b>Directly assigned:</b> Attests memberships that were assigned directly.</li> <li>• <b>By request:</b> Attests memberships that were requested.</li> <li>• <b>By delegation:</b> Attests memberships that were delegated.</li> </ul>

For this attestation procedure, you can use the following attestation policies:



Approval policies	Description
Attestation by selected approvers with automatic removal of assignments	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

## Attestation of memberships in business roles

Memberships in business roles are attested using the **Business role membership attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All roles	Attests memberships in all business roles.
Business roles with matching	Enter part of a name of business roles with memberships to attest. All business roles that have this pattern in their name are included.

Condition	Description
name	Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
Attesting by attestation status	<p>Select an attestation status Attests memberships in business roles that match this attestation status.</p> <p>You can select the follow status:</p> <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests memberships that have been denied.</li> <li>• <b>All Memberships:</b> Attests all memberships.</li> <li>• <b>New memberships:</b> Attests memberships that have never been attested.</li> </ul>
Specific employees	Select the identities. Attests identity memberships in business roles.
Specific employees with subidentities.	Select the identities. Attests identity memberships in business roles. In addition, this identity's subidentities memberships in business roles are attested.
Specific roles	<p>Select the business roles. Attests memberships in these business roles.</p> <p>Use  and  to switch between hierarchical and list view. Multi-select is possible.</p>
New or not attested for x days	Specify a number of days. Attests memberships in business roles that have not been attested for the defined number of days.
Roles with specific owners	Select the identities. Attests memberships in business roles of identities who are owners of these business roles.
Roles with specific role classes	Select the role classes. Attests membership in business roles of this role class.
Roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests memberships in business roles with a risk index in the chosen range.
Roles with any owner	Attests all memberships in business roles that have an owner.
Roles with owners in departments	Select the departments. Attests all business roles that have an owner in the selected department.
Roles by assignment type	<p>Select how memberships in business roles must be assigned to enable attestation:</p> <ul style="list-style-type: none"> <li>• <b>Directly assigned:</b> Attests memberships that were assigned directly.</li> </ul>

Condition	Description
	<ul style="list-style-type: none"> <li>• <b>By request:</b> Attests memberships that were requested.</li> <li>• <b>By delegation:</b> Attests memberships that were delegated.</li> <li>• <b>By dynamic role:</b> Attests memberships that were attested through dynamic roles.</li> </ul>

For this attestation procedure, you can use the following attestation policies:



Approval policies	Description
Attestation by selected approvers with automatic removal of assignments	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

## Attesting assignment of memberships in system roles

Memberships in system roles are attested using the **System role membership attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All roles	Attests memberships in all system roles.
System roles with matching name	Enter part of a name of system roles with memberships to attest. All system roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
Attesting by attestation status	Select an attestation status Attests memberships in system roles that match this attestation status. You can select the follow status: <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests memberships that have been denied.</li> <li>• <b>All Memberships:</b> Attests all memberships.</li> <li>• <b>New memberships:</b> Attests memberships that have never been attested.</li> </ul>
Specific roles	Select the system roles. Attests memberships in these system roles.

Condition	Description
	Use  and  to switch between hierarchical and list view. Multi-select is possible.
New or not attested for x days	Specify a number of days. Attests memberships in system roles that have not been attested for the defined number of days.
Roles with specific owners	Select the identities. Attests memberships in system roles of identities who are owners of these system roles.
Roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests memberships in system roles with a risk index in the chosen range.
Roles with any owner	Attests all memberships in system roles that have an owner.
Roles with owners in departments	Select the departments. Attests all system roles that have an owner in the selected department.
System roles by applications	Select the applications (Application Governance). Attests memberships in system roles assigned to these applications.
Roles by assignment type	<p>Select how memberships in system roles must be assigned to enable attestation:</p> <ul style="list-style-type: none"> <li>• <b>Directly assigned:</b> Attests memberships that were assigned directly.</li> <li>• <b>By request:</b> Attests memberships that were requested.</li> <li>• <b>Inherited:</b> Attests inherited memberships.</li> </ul>

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers with automatic removal of assignments	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

## Attesting device owners

Owners of devices are attested by using the **Device ownership attestation** attestation procedure.

Condition	Description
All devices	Attests owners of all the devices.

## Attesting system entitlement owners

Owners of system entitlements are attested by using the **System entitlement ownership attestation** attestation procedure.

Condition	Description
All system entitlements	Attests owners of all system entitlements.
System entitlements by applications	Select the applications. Attests system entitlements owners to which the applications are assigned.

## Attesting system entitlement owners (initial)

Initial assignments of product owners to system entitlements are attested using the **System entitlement ownership attestation (initial)** attestation procedure (this means that the system entitlements did not have an product owner beforehand).

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All system entitlements without owner	Attests initial assignments of owners to system entitlements that do not have product owners.
No dynamic groups from Active Roles	Attests initial assignment of product owners to system entitlements. Dynamic groups are ignored in the process.







For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation of ownership by proposed new owner	The proposed new product owners can make approval decisions about attestation cases.

# Attesting user accounts

User accounts are attested using the **User account attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:

Condition	Description
All user accounts	Attests all user accounts.
All privileged user accounts	Attests all privileged user accounts.
User accounts in the target system	Select the target systems. Attests user accounts assigned to these target systems.
User accounts of specific employees	Select the identities. Attests user accounts assigned to these identities.
Specific user accounts	Select the user accounts to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
User accounts with defined risk index	Specify a risk index range. Attests user accounts with a risk index in the chosen range.
User accounts with matching name	Enter part of a name of user accounts with access to attest. All user accounts that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
User accounts with employees in departments	Select the departments. Attests user accounts with identities assigned to these departments. Use  and  to switch between hierarchical and list view. Multi-select is possible.
User accounts of employees in child departments	Select the departments. Attests user accounts with identities assigned to these or their child departments. Use  and  to switch between hierarchical and list view. Multi-select is possible.
User accounts of employees with matching names	Enter part of a name of the identities with user accounts to attest. All identities that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests user accounts that have not been attested for the defined number of days.
All user accounts not assigned to an identity	Only attests user accounts not assigned to an identity (so-called orphaned user accounts).

Condition	Description
Linked user accounts	Attests only user accounts that are assigned these identities.
Target system type	Select the target systems types. Attests user accounts in target system of this target system type.



For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation by selected approvers	Click <b>Assign/Change</b> in the <b>Attestors</b> field and then select the identities that can make approval decisions about attestation cases.
Attestation by target system manager	Target system managers can be approved through attestation cases.

## Attesting system entitlements

System entitlements are attested using the **System entitlement attestation** attestation procedure.

For this attestation procedure you can use the following attestation conditions:



Condition	Description
All system entitlements	Attests all system entitlements.
Specific system entitlements	Select the system entitlements to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
No dynamic groups from Active Roles	Attests all system entitlements. Dynamic groups are ignored in the process.
System entitlements with defined risk index	Specify a risk index range. Attests system entitlements with a risk index in the chosen range.
System entitlements with matching name	Enter part of a name of system entitlements with access to attest. All system entitlements that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
System entitlements by applications	Select the applications. Attests system entitlements that are assigned to these applications.

For this attestation procedure, you can use the following attestation policies:

Approval policies	Description
Attestation of system entitlements by product owner (OA)	Product owners of system entitlements can be approved through attestation cases.
Attestation by target system manager	Target system managers can be approved through attestation cases.

## Attesting assignment of system entitlement to departments



System entitlements assignments to departments are attested using the **Attestation of system entitlement assignments to departments** attestation procedure.

Condition	Description
All departments	Attests assignments of system entitlements to all departments.
All system entitlements	Attests assignments of all system entitlements to departments.
Attesting by attestation status	Select an attestation status Attests assignments of system entitlements, matching this attestation status, to departments. You can select the follow status: <ul style="list-style-type: none"><li>• <b>Denied memberships:</b> Attests assignments that have been denied.</li><li>• <b>All Memberships:</b> Attests all assignments.</li><li>• <b>New memberships:</b> Attests assignments that have never been attested.</li></ul>
Specific departments	Select the departments with system entitlements to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific system entitlements	Select the with system entitlements with assignments to departments to attest.
Departments with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests system entitlement assignment assignments to departments with a risk index in the chosen range.
Departments with matching	Enter part of a name of departments with system entitlement assignments to attest. All departments that have this pattern in their

Condition	Description
name	name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system entitlement assignments to departments that have not been attested for the defined number of days.
System entitlements with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to departments.
System entitlements with matching name	Enter part of a name of system entitlements with assignments to departments to attest. All system entitlements that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting assignment of system entitlement to business roles

System entitlements assignments to business roles are attested using the **Attestation of system entitlement assignments to business roles** attestation procedure.



Condition	Description
All business roles	Attests assignments of system entitlements to all business roles.
All system entitlements	Attests assignments of all system entitlements to business roles.
Attesting by attestation status	Select an attestation status Attests assignments of system entitlements, matching this attestation status, to business roles. You can select the follow status: <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests assignments that have been denied.</li> <li>• <b>All Memberships:</b> Attests all assignments.</li> <li>• <b>New memberships:</b> Attests assignments that have never been attested.</li> </ul>
Specific business roles	Select the business roles with system entitlements to attest. Use  and  to switch between hierarchical and list view. Multi-select

Condition	Description
	is possible.
Specific system entitlements	Select the with system entitlements with assignments to business roles to attest.
Business roles with specific role classes	Select the role classes. Attests system entitlement assignments to business roles with these role classes.
Business roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests system entitlement assignments to business roles with a risk index in the chosen range.
Business roles with matching name	Enter part of a name of business roles with system entitlement assignments to attest. All business roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system entitlement assignments to business roles that have not been attested for the defined number of days.
System entitlements with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to business roles.
System entitlements with matching name	Enter part of a name of system entitlement with assignments to business roles to attest. All system entitlements that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attestation of system entitlement assignments to cost centers



System entitlements assignments to cost centers are attested using the **Attestation of system entitlement assignments to cost centers** attestation procedure.

Condition	Description
All cost centers	Attests assignments of system entitlements to all cost centers.
All system entitlements	Attests assignments of all system entitlements to cost centers.

Condition	Description
Attesting by attestation status	<p>Select an attestation status Attests assignments of system entitlements, matching this attestation status, to cost centers.</p> <p>You can select the follow status:</p> <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests assignments that have been denied.</li> <li>• <b>All Memberships:</b> Attests all assignments.</li> <li>• <b>New memberships:</b> Attests assignments that have never been attested.</li> </ul>
Specific cost centers	<p>Select the cost centers with system entitlements to attest.</p> <p>Use  and  to switch between hierarchical and list view. Multi-select is possible.</p>
Specific system entitlements	Select the with system entitlements with assignments to cost centers to attest.
Cost centers with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests system entitlement assignment assignments to cost centers with a risk index in the chosen range.
Cost centers with matching name	<p>Enter part of a name of cost centers with system entitlement assignments to attest. All cost centers that have this pattern in their name are included.</p> <p>Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.</p>
New or not attested for x days	Specify a number of days. Attests system entitlement assignments to cost centers that have not been attested for the defined number of days.
System entitlements with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to cost centers.
System entitlements with matching name	<p>Enter part of a name of system entitlement with assignments to cost centers to attest. All system entitlements that have this pattern in their name are included.</p> <p>Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.</p>



## Attestation of system entitlement assignments to locations

System entitlements assignments to locations are attested using the **Attestation of system entitlement assignments to locations** attestation procedure.

Condition	Description
All locations	Attests assignments of system entitlements to all locations.
All system entitlements	Attests assignments of all system entitlements to locations.
Attesting by attestation status	<p>Select an attestation status Attests assignments of system entitlements, matching this attestation status, to locations.</p> <p>You can select the follow status:</p> <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests assignments that have been denied.</li> <li>• <b>All Memberships:</b> Attests all assignments.</li> <li>• <b>New memberships:</b> Attests assignments that have never been attested.</li> </ul>
Specific locations	<p>Select the locations with system entitlements to attest.</p> <p>Use  and  to switch between hierarchical and list view. Multi-select is possible.</p>
Specific system entitlements	Select the with system entitlements with assignments to locations to attest.
Locations with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests system entitlement assignments to locations with a risk index in the chosen range.
Locations with matching name	<p>Enter part of a name of locations with system entitlement assignments to attest. All locations that have this pattern in their name are included.</p> <p>Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.</p>
New or not attested for x days	Specify a number of days. Attests system entitlement assignments to locations that have not been attested for the defined number of days.
System entitlements with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to locations.
System entitlements with matching name	<p>Enter part of a name of system entitlement with assignments to locations to attest. All system entitlements that have this pattern in their name are included.</p> <p>Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.</p>

# Attesting assignment of system role assignment to departments



System role assignments to departments are attested with the "Attestation of system role assignments to departments" attestation procedure.

Condition	Description
All departments	Assignments of system roles to all departments
All system roles	Attests assignments of all system roles to departments.
Attesting by attestation status	Select an attestation status Attests assignments of system roles, matching this attestation status, to departments. You can select the follow status: <ul style="list-style-type: none"><li>• <b>Denied memberships:</b> Attests assignments that have been denied.</li><li>• <b>All Memberships:</b> Attests all assignments.</li><li>• <b>New memberships:</b> Attests assignments that have never been attested.</li></ul>
Specific departments	Select the departments with system roles to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific system roles	Select the with system roles with assignments to departments to attest.
Departments with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests system role assignments to departments with a risk index in the chosen range.
Departments with matching name	Enter part of a name of departments with system role assignments to attest. All departments that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system role assignments to departments that have not been attested for the defined number of days.
System roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to departments.
System roles	Enter part of a name of system role with departments assignments to

Condition	Description
with matching name	attest. All system roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting assignment of system roles to business roles



System role assignments to business roles are attested with the "Attestation of system role assignments to business roles" attestation procedure.

Condition	Description
All business roles	Attests assignments of system roles to all business roles.
All system roles	Attests assignments of all system roles to business roles.
Attesting by attestation status	Select an attestation status Attests assignments of system roles, matching this attestation status, to business roles. You can select the follow status: <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests assignments that have been denied.</li> <li>• <b>All Memberships:</b> Attests all assignments.</li> <li>• <b>New memberships:</b> Attests assignments that have never been attested.</li> </ul>
Specific business roles	Select the business roles with system roles to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific system roles	Select the with system roles with assignments to business roles to attest.
Business roles with specific role classes	Select the role classes. Attests system roles assignments to business roles with these role classes.
Business roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests system role assignments to business roles with a risk index in the chosen range.
Business roles with matching name	Enter part of a name of business roles with system role assignments to attest. All business roles that have this pattern in their name are included.

Condition	Description
	Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system role assignments to business roles that have not been attested for the defined number of days.
System roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to business roles.
System roles with matching name	Enter part of a name of system role with business roles assignments to attest. All system roles that have this pattern in their name are included.  Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Cost center system role assignment attestation

System role assignments to cost centers are attested with the "Attestation of system role assignments to cost centers" attestation procedure.



Condition	Description
All cost centers	Attests assignments of system roles to all cost centers.
All system roles	Attests assignments of all system roles to cost centers.
Attesting by attestation status	Select an attestation status Attests assignments of system roles, matching this attestation status, to cost centers.  You can select the follow status: <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests assignments that have been denied.</li> <li>• <b>All Memberships:</b> Attests all assignments.</li> <li>• <b>New memberships:</b> Attests assignments that have never been attested.</li> </ul>
Specific cost centers	Select the cost centers with system roles to attest.  Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific	Select the with system roles with assignments to cost centers to attest.

Condition	Description
system roles	
Cost centers with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests system role assignments to cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with system role assignments to attest. All cost centers that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system role assignments to cost centers that have not been attested for the defined number of days.
System roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to cost centers.
System roles with matching name	Enter part of a name of system role with cost center assignments to attest. All system roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting assignment of system entitlements to locations

System role assignments to locations are attested with the "Attestation of system role assignments to locations" attestation procedure.

Condition	Description
All locations	Attests assignments of system roles to all locations.
All system roles	Attests assignments of all system roles to locations.
Attesting by attestation status	<p>Select an attestation status Attests assignments of system roles, matching this attestation status, to locations.</p> <p>You can select the follow status:</p> <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests assignments that have been denied.</li> <li>• <b>All Memberships:</b> Attests all assignments.</li> <li>• <b>New memberships:</b> Attests assignments that have never been attested.</li> </ul>

Condition	Description
Specific locations	Select the locations with system roles to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
Specific system roles	Select the with system roles with assignments to locations to attest.
Locations with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests system role assignments to locations with a risk index in the chosen range.
Locations with matching name	Enter part of a name of locations with system role assignments to attest. All locations that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests system role assignments to locations that have not been attested for the defined number of days.
System roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to locations.
System roles with matching name	Enter part of a name of system role with location assignments to attest. All system roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

## Attesting assignments to system roles

Assignments to system roles are attested using the **System role membership attestation** attestation procedure.

Condition	Description
All system roles	Attests assignments to all system roles.
Attesting by attestation status	Select an attestation status Attests assignments to system roles, matching this attestation status. You can select the follow status: <ul style="list-style-type: none"> <li>• <b>Denied memberships:</b> Attests assignments that have been denied.</li> <li>• <b>All Memberships:</b> Attests all assignments.</li> </ul>

Condition	Description
	<ul style="list-style-type: none"> <li>• <b>New memberships:</b> Attests assignments that have never been attested.</li> </ul>
Specific system roles	Select the with system roles with assignments to attest.
New or not attested for x days	Specify a number of days. Attests assignments to system roles that have not been attested for the defined number of days.
System roles by applications	Select the applications. Attests assignments to system roles assigned to these applications.
System roles with defined risk index	Use the <b>Lower limit</b> and <b>Upper limit</b> fields to define a risk index range. Attests assignments to system roles with a risk index in the chosen range.
System roles with matching name	Enter part of a name of system role with assignments to attest. All system roles that have this pattern in their name are included. Example: <b>Per</b> finds "Person", "Personal", "Perfection" and so on.

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

## Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

## Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at [www.YouTube.com/OneIdentity](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

## A

- add product to cart 26
- address book
  - display 16
- approval decision
  - display 54
- approval history
  - display 54
- approve
  - pending request 43
- attestation
  - by peer group 79
  - carry out 66
  - managing attestation policies 67
  - viewing completed attestations 66

## C

- change
  - language 19
- configure
  - request function 89
- cross-functional product 79

## D

- date format 19
- deactivate
  - email notification 19
- delete
  - shopping cart 33
- deny
  - pending request 43

## display

- approval decision 54
- approval history 54
- pending request 43
- shopping cart 28

## E

- edit
  - shelf details 95
- email notification
  - deactivate 19
  - enable 19
- enable
  - email notification 19

## G

- give reason 31
- grant approval
  - pending request 43

## H

- header 23

## I

- identity
  - add 81
  - edit 81
- identity as request template 34
- interest group 35

## L

language

change 19

log in 10

Password Reset Portal 11

log out 10, 12

login 10

## M

manage

shopping cart 27

subscription 20

menu bar 24

My Responsibilities

manage 81

## N

navigate 12

number format 19

## O

other identities' products 35

## P

password 16, 18

change 18

password question 16

change 16

create 16

delete 16

edit 16

manage 16

specify 16

unlock 16

Password Reset Portal

log in 11

peer group 34-35

peer group analysis

for attestation 79

pending request

approve 43

deny 43

display 43

grant approval 43

product

cross-functional 79

## R

reference user 34

request 26-27, 33

submit 33

request for multiple identities 32

request function

configure 89

set up 89

request history

display 50

request product 26-27, 33

from other identities 34

peer group 35

requests

act 26

about a reference user 34

for other recipient 36

other identities' products 34

edit pending request 42

extend 51

- failed 31
- invalid 31
- manage 25
- request group 37
- revoke 53

## **S**

- save for later 39
- saved for later 39-42
- serve 12
- set validity period 30
- setup
  - request function 89
- shelf details
  - edit 95
- shopping cart
  - clean up products 29
  - delete 29, 33
  - display 28
  - empty 29
  - fill 26
  - give reason 31
  - manage 27
  - move product to another shelf 39
  - request for multiple identities 32
  - save for later 39
  - saved for later 39-42
  - set validity period 30
  - specify priority 30
  - submit 28
- specify priority 30
- start page 23
- structure 23
- submit
  - shopping cart 28

- subscription
  - manage 20

## **U**

- user interface 23

## **V**

- value format 19