One Identity Starling CertAccess

Web Portal User Guide

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. 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.

Starling CertAccess Web Portal User Guide
Updated - 06 October 2021, 09:24

Contents

1

General tips and getting started

You can use the Web Portal to request and cancel products, and to renew current requests with limited lifetimes. If you own the respective entitlements, you can also approve requests and cancellations, and perform attestation.

> 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:
  - Internet Explorer 11 or later

    > NOTE: Starting February 1, 2022, One Identity Starling will no longer support Internet Explorer 11.
  - Firefox (release channel)
  - Chrome (release channel)
  - Safari (current version)
  - Microsoft Edge (release channel)

Detailed information about this topic

- Logging on and off on page 9
- Navigation and use on page 9
- Switching languages on page 13
- Enabling/disabling email notifications on page 13

- Report subscriptions management on page 14
- The user interface layout on page 16

Logging on and off

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.

Detailed information about this topic

- Logging off on page 9

Logging off

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

To log off from Web Portal

- In the header, click 👤 (**Profile**) > **Sign out**.

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 10
- Search on page 11
- Help on page 12
- Filtering on page 13

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 start page

Table 2: Overview of key combinations for navigating

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

Simple elements

Table 3: Overview of the controls used

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

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

Installed controls

Table 4: Overview of other controls

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

Search

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

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

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

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

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

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

Detailed information about this topic

- Context searching on page 12

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 12

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 Starling CertAccess 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.

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

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**.

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** page, in the **Language** dialog, select the language that you want to use for the Web Portal.
3. 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**).
4. 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** page, click **Email notifications**
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 14
- Editing report subscriptions on page 15
- Sending reports from report subscriptions on page 16
- Ending report subscriptions on page 16

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**.
2. On the **Report Subscriptions** page, click **Add subscription**.
3. 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.

4. Click **Next**.
5. 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.

6. Click **Next**.
7. 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**.

8. Click **Next**.
9. In the **Check and create subscription** step, check your data and change them if necessary by clicking on the respective step.
10. Click **Create**.

Editing report subscriptions

You can edit your existing report subscriptions.

To edit a report subscription

1. In the header, click 👤 (**Profile**) > **My report subscriptions**.
2. On the **Report Subscriptions** page, in the list, click **Edit** next to the report subscription that you want to edit.
3. 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**.

4. (Optional) In the details pane under **Parameter**, specify any other report specific settings. These settings might vary depending on what report you use.
5. 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 report subscriptions**.
2. 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.

Ending report subscriptions

You can unsubscribe from reports.

To end a report subscription

1. In the header, click 👤 (**Profile**) > **My report subscriptions**.
2. On the **Report Subscriptions** page, in the list, click ⋮ (**Actions**) > **Unsubscribe** next to the report subscription that you want to end.
3. 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

- Start page on page 17
- Header on page 17
- Menu bar on page 18

Start page

Open the start page by clicking **Start page** in the menu bar.

Once you have logged in successfully, the start page appears. Displayed across the start 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	Use these menu items to: • Log off • Change the language • Enable/disable email notifications • Manage report subscriptions
❓ Help	Here you can open the help. The help contains the entire contents of the Web Portal User Guide.

Menu bar

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

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

To open a menu

1. Click a menu in the menu bar.

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

2

Requests

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

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

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 31).
- You are notified whether your request is granted or denied.

> NOTE: Certain actions trigger a request in the Web Portal and are added to the cart. Theses actions are NOT, however, carried out over the **Requests** menu.

Detailed information about this topic

- Requesting products on page 19
- Saved for Later list on page 28
- Pending requests on page 31
- Displaying request history on page 38
- Canceling requests on page 38
- Renewing products with limit validity periods on page 39
- Unsubscribing products on page 41

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 20).
2. Verify the shopping cart and amend the product requests as required (see Managing products in the shopping cart on page 21).
3. Submit the request (see Submitting requests on page 27).

Detailed information about this topic

- Adding products to the shopping cart on page 20
- Managing products in the shopping cart on page 21
- Submitting requests on page 27
- Requesting products on the Saved for Later list on page 29
- Requesting for other identities on page 27

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 21). Then send the request (see Submitting requests on page 27).

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 21
- Submitting requests on page 27

Managing products in the shopping cart

After you have added products to your shopping cart (see Adding products to the shopping cart on page 20), you can delete individual product requests from the cart, add more details to them, or perform other actions.

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 22)
    - Define the validity of the products (see Setting the validity period of products in your shopping cart on page 23)

- Change the priority of the requests (see Specifying the priority of products in your shopping cart on page 24)
- Enter reasons for the requests (see Giving a reason for requests on page 24)
- Check the shopping cart for invalid products and remove them (see Checking the shopping cart on page 25)
- Request products for multiple identities (see Requesting products in the shopping cart for multiple identities on page 26)
- Place products on the Saved for Later list (see Saving products for later on page 28
- Show the Saved for Later list (see Displaying Saved for Later list on page 29)

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 27).

Related topics

- Adding products to the shopping cart on page 20
- Submitting requests on page 27
- Saved for Later list on page 28

Displaying the shopping cart

After you have added products to your shopping cart (see Adding products to the shopping cart on page 20), 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.

   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 20
- Submitting requests on page 27

Removing products from the shopping cart

After adding added products to your shopping cart (see Adding products to the shopping cart on page 20), 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 26.

Related topics

- Adding products to the shopping cart on page 20
- Submitting requests on page 27

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 20), 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 39.

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 20
- Submitting requests on page 27

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 20), 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 20
- Submitting requests on page 27

Giving a reason for requests

After you have added products to your shopping cart (see Adding products to the shopping cart on page 20), 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 20
- Submitting requests on page 27

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 20
- Submitting requests on page 27

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 20), 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 on page 27
- Adding products to the shopping cart on page 20
- Submitting requests on page 27

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 22
- Adding products to the shopping cart on page 20

Submitting requests

After you have added products to your shopping cart (see Adding products to the shopping cart on page 20), and edited and, if necessary, checked the request (see Managing products in the shopping cart on page 21), 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**.
3. In the **Submit Shopping Cart** dialog, confirm with **Yes**.

   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 25 and Removing products from the shopping cart on page 22).

   > NOTE: If a rule violation is found, the request continues to be processed but requires further approval from a manager.

Related topics

- Adding products to the shopping cart on page 20
- Managing products in the shopping cart on page 21
- Checking the shopping cart on page 25
- Removing products from the shopping cart on page 22

Requesting for other identities

You can make requests for other identities (such as department managers).

> 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 26.

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 **Employee** pane, in the list, select the check boxes next to the identities you want to request a product 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 20) that you want to request for the selected identities.
6. (Optional) Edit the shopping cart (see Managing products in the shopping cart on page 21).
7. Submit the request (see Submitting requests on page 27).

Related topics

- Requesting products in the shopping cart for multiple identities on page 26

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 28
- Displaying Saved for Later list on page 29
- Requesting products on the Saved for Later list on page 29
- Removing products from the Saved for Later list on page 30
- Deleting the Saved for Later list on page 31

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 29).

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 20).
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 21

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**.

   This opens the **Saved For Later** page.

Related topics

- Managing products in the shopping cart on page 21

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 21.
6. In the **Submit Shopping Cart** dialog, confirm with **Yes**.

Related topics

- Managing products in the shopping cart on page 21
- Submitting requests on page 27

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 31.

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 21

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 30.

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 21

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 32
- Approving and denying requests on page 32

- Appointing other approvers for pending requests on page 33
- Rejecting request approval on page 37

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 32).

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**.

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 33).
- Appoint additional approver
  You can give an another identity the task of approving (see Appointing additional approvers to pending requests on page 34). 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 37).
  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 35). 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 37).
  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 35

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 34

Delegating approvals of pending requests to other identities

You can delegate an approval decision about a request to another identity.

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 36

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 35

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 34

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 13). 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 38
- Renewing products with limit validity periods on page 39
- Unsubscribing products on page 41

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 13). 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**.

To cancel multiple requests

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 13). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to cancel requests belonging to another identity, in the 🔍 **Search** field, enter the identity's name.
6. Select the check boxes next to the requests you want to cancel.
7. Click ⋮ (**Actions**) > **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 cancelation.

   b. Click **Save**.

Related topics

- Requesting products on page 19
- Displaying request history on page 38
- Renewing products with limit validity periods on page 39
- Unsubscribing products on page 41

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 13). 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 13). 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 23
- Canceling requests on page 38
- Unsubscribing products on page 41

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 13). 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 13). 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 38
- Renewing products with limit validity periods on page 39
- Canceling requests on page 38

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 36
- Removing additional approvers of pending requests on page 35
- Approving and denying requests on page 32
- Undoing approvals on page 42

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 13). 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:
    1. In the **Reason for your decision**, enter why you want to undo the approval.
    2. Click **Save**.

Related topics

- Displaying approvals on page 42

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

- Pending attestations on page 45
- Displaying attestation history on page 53
- Attestation – Administration on page 54

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 45).

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 46
- Granting or denying attestation cases on page 46
- Appointing other approvers for pending attestation cases on page 47
- Rejecting approval of attestation cases on page 52

Displaying pending attestation cases

As attestor, you can display 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 object under **Attestation policy**.

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

Related topics

- Displaying attestation cases of application runs on page 65

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 object 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, enter a reason for your approval decision.

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

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

5. Click **Save**.

Related topics

- Displaying attestation cases of application runs on page 65

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 48).
- Appoint additional approver
  You can give an another identity the task of approving Appointing additional approvers to pending attestation cases on page 49). 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 52).
  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 51). 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 52).
  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 object 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 object under **Attestation policy**.
3. On the **Pending Attestations** page, in the list, select the check boxes next to the attestation cases whose approvals you want to reroute.
4. Click ⋮ (**Actions**) > **Reroute approval**.
5. In the **Reroute Approval** pane, in the **Select approval level** menu, select the respective approval level to reroute to.
6. (Optional) In the **Reason for your decision** field, enter a reason for rerouting.
7. Click **Save**.

Appointing additional approvers to pending attestation cases

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

To add an additional approver

1. In the menu bar, click **Attestation** > **Pending Attestations**.
2. 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 object 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 object 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 50

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 object 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 object 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 49

Delegating approvals of pending attestation cases to other identities

You can delegate an approval decision about an attestation case to another identity.

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 object 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 object 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 52

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 51

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 object 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 object 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 13). 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 52

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

Detailed information about this topic

- Attestation policies on page 54
- Starting attestation on page 63
- Attestation by peer group analysis on page 66

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 55
- Setting up attestation policies on page 56

- Editing attestation policies on page 58
- Copying attestation policies on page 61
- Deleting attestation policies on page 63
- Appendix: Attestation conditions and approval policies from attestation procedures on page 109

Displaying attestation policies

You can display enabled and disabled attestation policies.

To display attestation polices

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

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

Related topics

- Displaying attestation policies details on page 55

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 66

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. 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.

Property	Description
	NOTE: The selection of the attestation procedure is crucial. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The available options are modified to match the attestation procedure.
Approval policies	Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.
Attestors	Click **Assign**/**Change** and then select the identities that can make approval decisions about attestation cases. NOTE: This field is only shown if you have selected an attestation policy in the **Attestation policy** menu that demands attestation by an approver (for example, **Attestation by selected approvers**).
Calculation schedule	Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.
Time required (days)	Specifies how many day attestors have to make an approval decision about the attestation cases governed by this policy. If you do not want to specify a time, enter **0**.
Owner	Select the employee that takes responsibility 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.
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.

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

5. In the **Condition type** menu, click the condition type to use (see Appendix: Attestation conditions and approval policies from attestation procedures on page 109).

   > 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 109).
7. (Optional) Create more conditions if required. To do this, click **Add another condition**.
8. (Optional) If you have specified more than one condition, you must specify whether one or all of the conditions must be fulfilled by enabling the appropriate option:
   - **All conditions must be fulfilled**: The next time the attestation policy is run, new attestation cases are added for all objects fulfilling all of the conditions. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.
   - **At least one condition must be fulfilled**: The next time the attestation policy is run, new attestation cases are added for all objects that fulfill at least one of the conditions. Use of this option generates a superset of all the individual conditions of the selected objects.
9. Click **Create**.

Related topics

- Appendix: Attestation conditions and approval policies from attestation procedures on page 109

Editing attestation policies

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

To edit an attestation policy

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

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

   > NOTE: The system contains default attestation policies. These policies can only be edited to a limited degree. If you want to make changes to a default attestation policy, create a copy and edit the copy (see Copying attestation

policies on page 61).

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

Property	Description
automatically	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.

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 109).

   > 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 109).
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 109

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. Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Completed attestation cases can be deleted once the attestation policy is disabled.
Attestation policy	Enter a name for the attestation policy.
Description	Enter a description of the attestation policy.
Attestation procedure	Select which objects to attest with this attestation policy. NOTE: The selection of the attestation procedure is crucial. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The available options are modified to match the attestation procedure.
Approval policies	Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.
Attestors	Click **Assign**/**Change** and then select the identities that can make approval decisions about attestation cases.

Property	Description
	NOTE: This field is only shown if you have selected an attestation policy in the **Attestation policy** menu that demands attestation by an approver (for example, **Attestation by selected approvers**).
Calculation schedule	Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.
Time required (days)	Specifies how many day attestors have to make an approval decision about the attestation cases governed by this policy. If you do not want to specify a time, enter **0**.
Owner	Select the employee that takes responsibility 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.
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.

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 109).

   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 109).

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 109

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 **Include deactivated 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 58

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 64
- Sending reminders about attestation runs on page 45
- Extending attestation runs on page 66

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 45

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 Runs** tab.
4. (Optional) To further limit the attestation cases to be displayed, click ▼ (**Filter**) on the **Attestation cases** tab.
5. (Optional) To approve or reject 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 46
- Granting or denying attestation cases on page 46

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 56

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 45

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.

In a peer group analysis, attestation cases are automatically approved if at least 90% of the members of the peer group already have the membership to be attested. If this is not the case, attestation cases are automatically denied.

Related topics

- Appendix: Attestation conditions and approval policies from attestation procedures

Responsibilities

In Starling CertAccess, 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 68
- Ownerships on page 72

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 68

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 69
- Deactivating my identities on page 69
- Reactivating my identities on page 69

Displaying my identities

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

To display identities

1. In the menu bar, click **Home**.
2. On the start 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 start 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 start 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** section, clear the **Permanently deactivated** check box.
6. Click **Save**.

Attesting my identities

You can use attestation to test the balance between security and compliance within your company. Managers or others responsible for compliance can use the Starling CertAccess 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. Starling CertAccess uses the same workflows for recertification and attestation.

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

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

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

Detailed information about this topic

- Displaying attestation cases of my identities on page 70
- Approving and denying attestation cases of my identities on page 71

Displaying attestation cases of my identities

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

1. In the menu bar, click **Home**.
2. On the start 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 44
- Displaying pending attestation cases on page 46

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 start 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 44
- Granting or denying attestation cases on page 46

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 72

Assigning product owners to system entitlements

You can assign a product owner to a system entitlement that does not have one or assume ownership of it 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 45).

Managing data

The Web Portal provides you with comprehensive functionality for managing the following objects.

- Identities
- User accounts
- System entitlements

> NOTE: During a target system synchronization, not all the data exists and the list of data issues may be incomplete.

Detailed information about this topic

- Managing identities on page 73
- Managing user accounts on page 77
- Managing system entitlements on page 79
- Display and resolving data issues on page 86
- Deleting data on page 87
- Generating reports on page 88

Managing identities

You can use the Web Portal to display, edit, or delete identities.

Detailed information about this topic

- Displaying identities on page 74
- Assigning managers to identities on page 74
- Deactivating identities on page 74
- Reactivating identities on page 75
- Deleting identities on page 75

Displaying identities

You can display any of the identities and their details.

To display identities

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identites**.

   This opens the **Identities** view and displays all the identities.
3. (Optional) To display details of an identity, click it in the list.

   | TIP: To create a report about an identity, click **Download report**.

Related topics

- Generating reports on page 88

Assigning managers to identities

You can assign managers to identities or remove the currently assigned manager.

To assign a manager to an identity

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. In the list, click the identity that you want to assign a new manager to.
4. In the details pane, perform one of the following actions:
   - In the **Manager** menu, click the manager you want to assign to the identity.
   - To remove the current manager, click ✕ (**Remove assignment**).
5. Click **Save**.

Related topics

- Display and resolving data issues on page 86

Deactivating identities

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

Effects of permanent deactivating an identity are:

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

To deactivate an identity

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. In the list, click the identity that you want to reactivate.
4. In the details pane, set the toggle to **Deactivated**.
5. Click **Save**.

Reactivating identities

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

To reactivate an identity

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. In the list, click the identity that you want to activate.
4. In the details pane, set the toggle to **Activated**.
5. Click **Save**.

Deleting identities

When an identity is deleted, they are tested to see if user accounts and company resources are still assigned, or if there are still pending requests. The identity is marked for deletion and therefore locked out of further processing. Before an identity is permanently deleted from the database, you must remove all company resource assignments and finalize all requests. If no more company resources are assigned, the identity is deleted permanently.

To delete an identity

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.

3. In the list, click the identity that you want to delete.
4. In the details pane, click **Delete**.

Managing attestation cases of identities

You can use the Web Portal to display all the attestation cases for identities and make approval decisions about them.

Detailed information about this topic

- Displaying attestation cases of identities on page 76
- Approving and denying attestation cases of identities on page 76

Displaying attestation cases of identities

You can display all the identities' attestation cases. In addition, you can obtain more information about the attestation cases.

To display attestation cases of an identity

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. In the list, 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 44
- Displaying pending attestation cases on page 46

Approving and denying attestation cases of identities

You can grant or deny approval to attestation cases of identities.

To approve an attestation case

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. In the list, click the identity whose attestation cases you want to decide approval on.
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 44
- Granting or denying attestation cases on page 46

Managing user accounts

You can use the Web Portal to display, edit, or delete user accounts.

Detailed information about this topic

- Displaying user accounts on page 77
- Displaying user account memberships on page 79
- Synchronizing user account managers on page 79

Displaying user accounts

You can display any of the user accounts and their details.

To display user accounts

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **User accounts**.

   This opens the **User accounts** view and displays all the user accounts.
3. (Optional) To display details of a user account, click it in the list.

   TIP: To create a report about a user account, click **Download report**.

Related topics

- Generating reports on page 88

Editing user accounts

You can edit user accounts.

To edit a user account

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **User accounts**.
3. In the list, click the user account you want to edit.
4. In the details pane, edit the user account's main data.

   Table 10: Service item main data

Property	Description
Identity	Select the identity to which the user account should be linked.
Not linked to an identity	Select the check box if the user account does not need to be linked with any identity (for example, if multiple identities use the user account). In this case, the user account is no longer treated as an "orphaned" user account. Orphaned user accounts are user accounts that are not linked with any identity.
Synchronize the user account's manager with the listed identity	Set the switch to assign the same manager to the user account that is assigned to the linked identity (see Synchronizing user account managers on page 79).

5. Click **Save**.

Displaying user account memberships

You can display which system entitlements are assigned to user accounts.

To display memberships

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **User accounts**.
3. In the list, click the user account whose memberships you want to display.
4. In the details pane, click the **Memberships** tab.

   > TIP: If you click a system entitlement in the list, you will see more information and options (see Managing system entitlements on page 79).

Synchronizing user account managers

If the manager of a user account does not match the manager of the identity assigned to the user account, you can align the managers. In this case, the user account is assigned the manager that is assigned to the associated identity.

To synchronize a user account's manager

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **User accounts**.
3. In the list, click the user account whose manager you want to align.
4. In the details pane, set **Synchronize the user account's manager with the listed identity**.
5. Click **Save**.

Managing system entitlements

You can use the Web Portal to display, edit, or delete system entitlements.

System entitlements map the objects that control access to target system resources in the target systems. A user account obtains the required permissions for accessing target system resources through its memberships in system entitlements.

Detailed information about this topic

- Displaying system entitlements on page 80
- Displaying system entitlement memberships on page 80

- Editing risk indexes of system entitlements on page 81
- Editing service items for system entitlements on page 83
- Making system entitlements requestable on page 93

Displaying system entitlements

You can display any of the system entitlements and their details.

To display system entitlements

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.

   This opens the **System Entitlements** view and displays all the system entitlements.
3. (Optional) To display details of a system entitlement, click it in the list.

   TIP: To create a report about a system entitlement, click **Download report**.

Related topics

- Generating reports on page 88

Displaying system entitlement memberships

You can display which user accounts are assigned to system entitlements.

To display memberships

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. In the list, click the system entitlement whose memberships you want to display.
4. In the details pane, click the **Memberships** tab.
5. (Optional) To display all directly assigned memberships, click **Directly assigned**.
6. (Optional) To display all indirectly assigned memberships, click **Indirectly assigned**.

Deleting system entitlement memberships

You can delete memberships of user accounts in system entitlements.

To delete memberships

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. In the list, click the system entitlement with membership that you want to delete.
4. In the details pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Directly assigned**.
6. Select the check box next to the membership you want to delete.
7. Click **Delete**.

Editing risk indexes of system entitlements

You can edit the risk indexes of system entitlements. The risk index is used to assess the risk of assigning system entitlements to user accounts.

To edit the risk index

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. In the list, click the system entitlement whose risk index you want to edit.
4. In the details pane, under **Risk index**, define the risk index using the slider.
5. Click **Save details**.

Creating service items for system entitlements

In order for system entitlements to be requested as products, they are assigned to corresponding service items. You can create service items for system entitlements.

To create a service item for a system entitlement

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. In the list, click the system entitlement for which you want to create a service item.
4. In the details pane, click the **Details** tab.
5. On the **Details** tab, click **Create service item**.
6. Click **Service Item** tab.

7. On the **Service Item** tab, edit the service item's main data.

Table 11: Service item main data

Property	Description
Description	Enter a description of the system entitlement.
Service category	You can group different service items into service categories. To do this, click **Assign**/**Change** and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 103.
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Attestors	Click **Assign**/**Change** and then select an application role. Members of this application role can approve attestation cases that affect the service item.
Not requestable/Requestable	Set the switch to **Requestable** if you want to request system entitlements through the Web Portal. Set the switch to **Not requestable** if you do not want to request system entitlements through the Web Portal. For more information, see Making system entitlements requestable on page 93.
Product owners	Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item. To specify members of an application role as the product owner, enable the **Select from roles** option, next to the **Product owner** field, click **Assign**/**Change**, then select the appropriate application role. To specify a certain identity as the product owner, enable the **Select from identities** option and then select the corresponding identity in the **Identity** menu.

8. Click **Save service item**.

Editing service items for system entitlements

In order for system entitlements to be requested as products, they are assigned to corresponding service items. You can edit the main data of these service items.

To display and edit a service items role's main data

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. In the list, click the system entitlement whose service item you want to edit.
4. In the details pane, click the **Service item** tab.

5. On the **Service Item** tab, edit the service item's main data.

Table 12: Service item main data

Property	Description
Description	Enter a description of the system entitlement.
Service category	You can group different service items into service categories. To do this, click **Assign/Change** and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 103.
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Attestors	Click **Assign/Change** and then select an application role. Members of this application role can approve attestation cases that affect the service item.
Not requestable/Requestable	Set the switch to **Requestable** if you want to request system entitlements through the Web Portal. Set the switch to **Not requestable** if you do not want to request system entitlements through the Web Portal. For more information, see Making system entitlements requestable on page 93.
Product owners	Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item. To specify members of an application role as the product owner, enable the **Select from roles** option, next to the **Product owner** field, click **Assign/Change**, then select the appropriate application role. To specify a certain identity as the product owner, enable the **Select from identities** option and then select the corresponding identity in the **Identity** menu.

6. Click **Save service item**.

Related topics

- Assigning product owners to system entitlements on page 72

Managing attestation cases of system entitlements

You can use the Web Portal to display all the attestation cases for system entitlements and make approval decisions about them.

Detailed information about this topic

- Displaying attestation cases of system entitlements on page 85
- Approving and denying attestation cases of system entitlements on page 85

Displaying attestation cases of system entitlements

You can display all the system entitlements' attestation cases. In addition, you can obtain more information about the attestation cases.

To display attestation cases of a system entitlement

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. In the list, click the system entitlement whose attestation cases you want to display.
4. In the details pane, click the **Attestation** tab.

   This displays all the system entitlement's attestation cases.
5. (Optional) To display more details of an attestation case, click **Details** next to the attestation case.

Related topics

- Attestation on page 44
- Displaying pending attestation cases on page 46

Approving and denying attestation cases of system entitlements

You can grant or deny approval to attestation cases of system entitlements.

To approve an attestation case

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. In the list, click the system entitlement whose attestation case you want to decide approval on.
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 44
- Granting or denying attestation cases on page 46

Display and resolving data issues

If problems, differences, or inconsistencies occur with respect to your data, you can display them and, if necessary, resolve them.

You can start an attestation for identities that do not have a manager. In the process of attesting, these identities can specify who their manager is.

> NOTE: During a target system synchronization, the list of data issues may be incomplete.

To display issues

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer, click ⚠ **Issues found**.
3. On the **Data Readiness** page, perform the following actions:

- To display the identities that do not have a manager assigned to them, click **View** next to **<count> identities need a manager**.
- To display the user accounts that do not have an identity assigned to them, click **View** next to **<count> user accounts need an identity**.
- To display the system entitlements that do not have a product owner assigned to them, click **View** next to **<count> system entitlements need an owner**.
- If there are not any system entitlements marked as requestable, you can display the system entitlements in order to make them requestable (see Making system entitlements requestable on page 93). Click **View** next to **There are no requestable system entitlements**.

To assign a manager to all identities without a manager

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer, click ⚠ **Issues found**.
3. Next to **Identities**, click **Fix**.
4. In the **Start attestation** dialog, click **Start**.

   This starts an attestation and creates an attestation case for each of the respective identities. As part of this attestation, these identities can specify who their manager is.

Related topics

- Assigning managers to identities on page 74

Deleting data

You can delete all the data in a domain. For example, this might be necessary if want to import everything again in order to have a clean set of data.

> NOTE: You can only delete data from a domain if synchronization is set up for the domain in the Starling CertAccess Agent. If you still want to delete domain data, remove the synchronization in the Starling CertAccess Agent first.

To display issues

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer, click 🗑 **Delete data**.
3. In the **Delete data** dialog, in the **Delete domain** menu, select the domain whose data you want to delete.
4. Click **Delete all data**.

   > NOTE: Deleting the data may take some time.

Generating reports

You can generate comprehensive reports for identities, user accounts, system entitlements.

To generate a report

1. In the menu bar, click **Data** > **Reports**.
2. On the Reports page, perform the following:
   - To generate a report about identities, enable **identities**.
   - To generate a report about user accounts, enable **User accounts**.
   - To generate a report about system entitlements, enable **System entitlements**.
3. In the **Select a report** menu, filter the list by selecting a report. Depending on what you selected in the previous step, the reports (with more parameters) on offer will vary:
   - Reports for identities
     - **Specific identity**: Generates a report about a specific identity.
       Next, in the **Select an identity** menu, select the identity that you want to generate the report about.

       > TIP: When you display details of an identity in the Data Explorer, you can generate a report about it as well (see Displaying identities on page 74).
     - **Identities reporting to a specific identity**: Generates a report about all the identities that report directly to a specific identity.
       Next, in the **Select an identity** menu, select an identity. All the identities that report to this identity are taken into account in the report.
   - Reports for user accounts
     - **Specific user account**: Generates a report about a specific user account.
       Next, in the **Select a user account** menu, select the user account that you want to generate the report about.

       > TIP: When you display details of a user account in the Data Explorer, you can generate a report about it as well (see Displaying user accounts on page 77).
     - **User accounts owned by a specific identity**: Generates a report about all the user accounts that report directly to a specific identity.
       Next, in the **Select an identity** menu, select an identity. All user accounts owned by this identity are taken into account in the report.
     - **User accounts where an identity is managed by a specific identity**: Generates a report about all the user accounts assigned to an identity that reports directly to a specific identity.
       Next, in the **Select an identity** menu, select an identity. All the user

accounts of the identity that reports directly to the selected identity, are taken into account.

    - **User accounts in a domain**: Generates a report about all the user accounts that are assigned to a specific domain.
      Next, in the **Select a domain** menu, select a domain. All the user accounts that are assigned to this domain are taken into account in the report.
    - **User accounts in a container**: Generates a report about all the user accounts that are assigned to a specific container.
      Next, in the **Select a container** menu, select a container. All the user accounts that are assigned to this container are taken into account in the report.

  - Reports for system entitlements
    - **Specific system entitlement**: Generates a report about a specific system entitlement.
      Next, in the **Select a system entitlement** menu, select the system entitlement that you want to generate the report about.

      > TIP: When you display details of a system entitlement in the Data Explorer, you can generate a report about it as well (see Displaying system entitlements on page 80).

    - **System entitlements in a domain**: Generates a report about all the system entitlements that are assigned to a specific domain.
      Next, in the **Select a domain** menu, select a domain. All the system entitlements that are assigned to this domain are taken into account in the report.
    - **System entitlements in a container**: Generates a report about all the system entitlements that are assigned to a specific container.
      Next, in the **Select a container** menu, select a container. All the system entitlements that are assigned to this container are taken into account in the report.
    - **System entitlements owned by a specific identity**: Generates a report about all the system entitlements that report directly to a specific identity.
      Next, in the **Select an identity** menu, select an identity. All system entitlements owned by this identity are taken into account in the report.

4. In the **Period to be considered (in days)**, enter how many of the previous days to take into account in the report. For example, if you enter **15** here, the last 15 days are taken into account.
5. Click **Generate report**.

Related topics

- Managing identities on page 73
- Managing user accounts on page 77
- Managing system entitlements on page 79

6

Managing user permissions for the Web Portal

Application roles help control Web Portal users permissions. Identities become members in application roles and obtain their permissions through them.

Application roles have the following aims:

- Program functions, identities, company resources, approval workflows and approval policies are assigned to fixed application roles. Permissions for these application roles must not be defined specifically for the company. This simplifies how you manage permissions.
- Enables audit secure internal administration of Starling CertAccess users and their permissions. Permissions can be granted through assignment, request, and approval or by calculation on account of specific properties. The plausibility of the permissions can be tested at any time with the attestation function.
- Users are provided with initial permissions, which they require for carrying out their tasks. For example, this is a way to create initially required user accounts.

Detailed information about this topic

- Displaying application roles on page 90
- Assigning application roles to identities on page 91
- Removing identities from application roles on page 91

Displaying application roles

You can display any application roles and their members.

To display an application role

1. In the menu bar, click **Setup** > **Application roles**.

   This opens the **Application Roles** page.

2. (Optional) To display the members of an application role, in the list, click the application role.

Assigning application roles to identities

You can assign application roles to identities by adding the identities to application roles as members. Once an identity becomes a member in an application role, it obtains its respective permissions.

> NOTE: To add a member to an application role, you must be a member in the respective application role yourself.

To add a member to an application role

1. In the menu bar, click **Setup** > **Application roles**.
2. On the **Application Roles** page, click the application role that you want to add a member to.
3. In the **Edit Application Role** pane, click **Add members**.
4. In the dialog, select the check box in front of the identity that you want to add to the application role as a member.
5. Click **Apply**.

Removing identities from application roles

You can remove identities from application roles by removing the identities' membership in the application roles. Once an identity is no longer a member in an application, it loses its respective permissions.

> NOTE: To be able to remove a member from an application role, the member must have been added directly to the application role (use the following steps) or you have requested the appropriate membership.

To remove a member from an application role

1. In the menu bar, click **Setup** > **Application roles**.
2. On the **Application Roles** page, click the application role that you want to remove a member from.
3. In the **Edit Application Role** pane, select the check box next to the member that you want to remove.
4. Click **Remove**.

Setting up and configuring request functions

In order to request system entitlements 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

The request shop is the top element in the hierarchical structure that is required for requesting system entitlements. A request shop can contain several shelves. Requestable system entitlements are then assigned to these shelves.

System entitlements can be grouped by 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 specify which approval procedure to use by assigning approval procedures to request shops, shelves or individual system entitlements (see Editing details of request shops on page 96, Editing shelf details on page 98, and Editing service items for system entitlements on page 83).

Detailed information about this topic

- Making system entitlements requestable on page 93
- Managing request shops on page 93
- Managing service categories on page 103

Making system entitlements requestable

To be able to request a system entitlements in the Web Portal, the system entitlement must fulfill the following prerequisites:

- The system entitlement must be assigned to a service item .
- The system entitlement must be marked as requestable (see following step-by-step).
- The system entitlement must be assigned to a shelf in a request shop (see Adding system entitlements to shelves on page 102).

To make a system entitlement requestable

1. In the menu bar, click **Data** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. (Optional) To display only those system entitlements only that are not marked as requestable, perform the following actions:
    a. Click ▼ (**Filter**).
    b. In the filter context menu, select the **Not requestable** check box.
4. In the list, select the check box in front of the system entitlement that you want to make requestable.
5. Under the list, set the switch to **Make selected items requestable** and click **Update**.

    > TIP: If you do not want the system entitlement to be requested in the Web Portal anymore, set the switch to **Make selected items not requestable**.

6. Assign the system entitlement to a shelf in the request shop that you want to use later to request it from (see Adding system entitlements to shelves on page 102).

Related topics

- Managing request shops on page 93
- Editing service items for system entitlements on page 83
- Adding system entitlements to shelves on page 102

Managing request shops

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

The request shop is the top element in the hierarchical structure that is required for requesting system entitlements.

A request shop can contain several shelves (see Managing request shop shelves on page 97). Requestable system entitlements are then assigned to these shelves (see Managing requestable system entitlements in request shops on page 101).

Detailed information about this topic

- Displaying request shops on page 94
- Creating request shops on page 94
- Editing request shops on page 95
- Deleting request shops on page 96
- Managing request shop shelves on page 97
- Managing access to requestable system entitlements in request shops on page 100
- Managing requestable system entitlements in request shops on page 101

Displaying request shops

You can display any of the request shops and their details.

To display request shops

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

   This opens the **Request Shops** page.
2. (Optional) To display details of a request shop, click on the request shop in the list.
3. (Optional) You can perform the following actions:
   - You can display the request shop's shelves (see Displaying request shop shelves on page 97).
   - You can see who can request system entitlements from the request shop (see Displaying members of request shops on page 100).

Creating request shops

To set up your own request shop solution, you can create request shops. Once created, you can customize these request shops as you wish (see Editing request shops on page 95).

To create a request shop

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, click **Create request shop**.

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

Table 13: Request shop main data

Property	Description
Name	Enter a full, descriptive name for the request shop.
Description	Enter a description for the request shop.
Attestors	Click **Assign**/**Change** and select an application role. Members of this application role can approve attestation cases affecting system entitlements that can be requested through this request shop. This setting is usual inherited by all the shelves that are assigned to this request shop and do not have an attestor.
Approval policies	Click **Assign**/**Change** and select the approval policies that control how approvers are determined if system entitlements are requested from this request shop in the Web Portal. This setting is usual inherited by all the shelves that are assigned to this request shop and do not have an approval policy.

4. Click **Create**.
5. (Optional) Create shelves for the request shop (see Creating shelves for request shops on page 97). In the shelves, you can specify which system entitlements can be requested from the request shop (see Adding system entitlements to shelves on page 102).
6. (Optional) To specify who can request system entitlements from the request shop, add members to the request shop (see Adding members to request shops on page 100).

Editing request shops

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

- Edit request shop details (see Editing details of request shops on page 96)
- Manage request shop shelves (see Managing request shop shelves on page 97)
- Specify who can request system entitlements from request shops (see Managing access to requestable system entitlements in request shops on page 100)
- Specify which system entitlements can be requested from request shops (see Managing requestable system entitlements in request shops on page 101)

Editing details of request shops

You can edit details of existing request shops.

To edit details of a request shop

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, in the list, click the request shop whose details you want to edit.
3. In the details pane, edit the request shop's main data.

Table 14: Request shop main data

Property	Description
Name	Enter a full, descriptive name for the request shop.
Description	Enter a description for the request shop.
Attestors	Click **Assign/Change** and select an application role. Members of this application role can approve attestation cases affecting system entitlements that can be requested through this request shop. This setting is usual inherited by all the shelves that are assigned to this request shop and do not have an attestor.
Approval policies	Click **Assign/Change** and select the approval policies that control how approvers are determined if system entitlements are requested from this request shop in the Web Portal. This setting is usual inherited by all the shelves that are assigned to this request shop and do not have an approval policy.

4. Click **Save**.

Deleting request shops

You can delete request shops.

> NOTE: Before you can delete a request shop, you must delete all the shelves from it (see Deleting request shop shelves on page 99) and remove all the members (see Removing members from request shops on page 101).

To delete a request shop

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

Managing request shop shelves

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

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

Detailed information about this topic

- Displaying request shop shelves on page 97
- Creating shelves for request shops on page 97
- Editing request shop shelves on page 98
- Editing shelf details on page 98
- Deleting request shop shelves on page 99

Displaying request shop shelves

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

To display the shelves in a request shop

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, in the list, click the request shop whose shelves you want to display.
3. In the details pane, click the **Shelves** tab.
4. (Optional) To display details of a shelf, click it in the list.
5. (Optional) You can display the system entitlements that can be requested over this shelf (see Displaying requestable system entitlements on page 101).

Creating shelves for request shops

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

To create a shelf for request shop

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, in the list, click the request shop you want to create a shelf for.
3. In the details 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 15: Shelves main data

Property	Description
Name	Enter a full, descriptive name for the shelf.
Description	Enter a description for the shelf.
Attestors	Click **Assign/Change** and select an application role. Members of this application role can approve attestation cases affecting system entitlements that can be requested through this shelf. This setting is inherited by all the system entitlements that are assigned to this shelf and do not have an attestor.
Approval policies	Click **Assign/Change** and select the approval policies that control how approvers are determined if system entitlements are requested from this shelf in the Web Portal. This setting is inherited by all the system entitlements that are assigned to this shelf and do not have an approval policy.

6. Click **Create**.
7. (Optional) To specify which system entitlements can be requested from the shelf, add the system entitlements to the shelf (see Adding system entitlements to shelves on page 102).

Editing request shop shelves

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

- Edit shelf details (see Editing details of request shops on page 96)
- Specify which system entitlements can be requested from request shops (see Managing requestable system entitlements in request shops on page 101)

Editing shelf details

You can edit details of existing shelves.

To edit details of a shelf

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, in the list, click the request shop whose shelf you want to edit.
3. In the details pane, click the **Shelves** tab.
4. On the **Shelf** tab, in the list, click the shelf you want to edit.

5. In the details pane, edit the shelf's main data.

Table 16: Shelves main data

Property	Description
Name	Enter a full, descriptive name for the shelf.
Description	Enter a description for the shelf.
Attestors	Click **Assign/Change** and select an application role. Members of this application role can approve attestation cases affecting system entitlements that can be requested through this shelf. This setting is inherited by all the system entitlements that are assigned to this shelf and do not have an attestor.
Approval policies	Click **Assign/Change** and select the approval policies that control how approvers are determined if system entitlements are requested from this shelf in the Web Portal. This setting is inherited by all the system entitlements that are assigned to this shelf and do not have an approval policy.

6. Click **Save**.

Related topics

- Managing requestable system entitlements in request shops on page 101

Deleting request shop shelves

You can delete request shop shelves.

> NOTE: Before you can delete a shelf, you must remove all the system entitlements from it (see Removing system entitlements from shelves on page 103).

To delete a shelf from a request shop

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

Managing access to requestable system entitlements in request shops

You can decide who is able to request system entitlements from request shops. This you specify through memberships in the request shop. Once an identity becomes a member of a request shop, they can request system entitlements from it.

Detailed information about this topic

- Displaying members of request shops on page 100
- Adding members to request shops on page 100
- Removing members from request shops on page 101

Displaying members of request shops

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

To display members of a request shop

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, in the list, click the request shop whose members you want to display.
3. In the details pane, click the **Access** tab.

Adding members to request shops

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

To add a member to a request shop

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

Removing members from request shops

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

To remove a member from a request shop

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, in the list, click the request shop you want to remove a member from.
3. In the details 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 system entitlements in request shops

You can decide which system entitlements can be requested from request shops. Once system entitlements have been allocated to shelves in a request shop (see Adding system entitlements to shelves on page 102) and marked as requestable (see Making system entitlements requestable on page 93), they can be requested in the Web Portal by members of the request shop.

Detailed information about this topic

- Displaying requestable system entitlements on page 101
- Adding system entitlements to shelves on page 102
- Editing requestable system entitlements on page 102
- Removing system entitlements from shelves on page 103

Displaying requestable system entitlements

You can display which system entitlements can be requested from request shops over shelves.

To display a shelf's requestable system entitlements

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, click the request shop in the list whose requestable system entitlements you want to display.

3. In the details pane, click the **Shelves** tab.
4. On the **Shelves** tab, in the list, click the shelf with the requestable system entitlement you want to display.
5. In the details pane, click the **System Entitlements** tab.
6. (Optional) To display more details about a system entitlement, on the **System Entitlements** tab, click the system entitlement. For more information, see Managing system entitlements on page 79.

Adding system entitlements to shelves

You can add system entitlements to shelves. Once system entitlements have been allocated to shelves in a request shop and marked as requestable (see Making system entitlements requestable on page 93), they can be requested in the Web Portal by members of the request shop.

To add a system entitlement to a shelf

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, in the list, click the request shop that you want request the system entitlement from later.
3. In the details 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 details pane, click the **System Entitlements** tab.
6. On the **System Entitlements** tab, click **Add system entitlements**.
7. In the dialog, select the check box in front of the system entitlement that you want to add to the shelf.
8. Click **Apply**.

Editing requestable system entitlements

You can edit system entitlements that can be requested over request shop shelves.

To edit a shelf's requestable system entitlements

1. In the menu bar, click **Setup** > **Request shops**.
2. On the **Request Shops** page, click the request shop in the list whose system entitlements you want to edit.
3. In the details pane, click the **Shelves** tab.
4. On the **Shelves** tab, in the list, click the shelf with the requestable system entitlement you want to edit.
5. In the details pane, click the **System Entitlements** tab.

6. On the **System Entitlements** tab, in the list, click the system entitlement you want to edit.
7. In the details pane, edit the system entitlement (see Managing system entitlements on page 79).

Removing system entitlements from shelves

You can remove system entitlements from shelves. the system entitlements cannot be requested anymore from this shelf.

To remove a system entitlement from a shelf

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

Managing service categories

Use the Web Portal to display and edit service categories.

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

You can assign system entitlements' service items to these service categories (see Editing service items for system entitlements on page 83).

Detailed information about this topic

- Displaying service categories on page 104
- Creating service categories on page 104
- Editing service categories on page 106
- Deleting service categories on page 108

Displaying service categories

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

To display service categories

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

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

2. (Optional) To display details of a service category, click it in the list.

Creating service categories

You can create service categories.

To create a service category

1. On the menu bar, click **Setup** > **Service categories**.
2. On the **Service Categories** page, click **Create service category**.

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

Table 17: Service category main data

Property	Description
Service category	Enter a full, descriptive name for the service category.
Description	Enter a description for the service category.
Parent service category	To structure service categories hierarchically, click **Assign**/**Change** and then select the parent service category.
Attestors	Click **Assign**/**Change** and then select an application role. Members of this application role can approve attestation cases that affect the service category.
Product owners	Click **Assign**/**Change** and then select an application role. Members of this application role can edit the service category's main data. They can also be used as approvers in approval processes when requests for service items assigned to this service category.
Approval policies	Select the approval policy used to determine the approver when the service item is requested in the Web Portal. NOTE: The approval policy specified for a service category is inherited by all associated service items and all child service categories where this is not specified.
Sort order	Enter the way you want the service category's service items to be sorted.
Picture	Add a picture of the service category. Users see this picture when they make a request. NOTE: The service category's picture is inherited by all associated service categories and service items that do not have one themselves. Perform the following actions to do this: 1. Click **Add**/**Change**. 2. In the **Picture** dialog box, click **Select Image**. 3. Select an image from your medium. 4. Click **Save**.
Service items	Specify the products can be requested through the service category. Perform the following actions to do this:

Property	Description
	1. Click **Assign**/**Change**. 2. Select the check box in front of the service item you want to assign to the service category. TIP: To remove a service item, deselect the relevant check box in front of the service item. To remove all service items, click **Clear selection**. 3. Click **Apply**.

4. Click **Save**.

Editing service categories

You can edit service items.

To edit a service category

1. On the menu bar, click **Setup** > **Service categories**.
2. On the **Service Categories** page, in the list, click the service category you want to edit.

3. In the details pane, edit the service category's main data.

Table 18: Service category main data

Property	Description
Service category	Enter a full, descriptive name for the service category.
Description	Enter a description for the service category.
Parent service category	To structure service categories hierarchically, click **Assign**/**Change** and then select the parent service category.
Attestors	Click **Assign**/**Change** and then select an application role. Members of this application role can approve attestation cases that affect the service category.
Product owners	Click **Assign**/**Change** and then select an application role. Members of this application role can edit the service category's main data. They can also be used as approvers in approval processes when requests for service items assigned to this service category.
Approval policies	Select the approval policy used to determine the approver when the service item is requested in the Web Portal. NOTE: The approval policy specified for a service category is inherited by all associated service items and all child service categories where this is not specified.
Sort order	Enter the way you want the service category's service items to be sorted.
Picture	Add a picture of the service category. Users see this picture when they make a request. NOTE: The service category's picture is inherited by all associated service categories and service items that do not have one themselves. Perform the following actions to do this: 1. Click **Add**/**Change**. 2. In the **Picture** dialog box, click **Select Image**. 3. Select an image from your medium. 4. Click **Save**.
Service items	Specify the products can be requested through the service category. Perform the following actions to do this:

Property	Description
	1. Click **Assign**/**Change**. 2. Select the check box in front of the service item you want to assign to the service category. TIP: To remove a service item, deselect the relevant check box in front of the service item. To remove all service items, click **Clear selection**. 3. Click **Apply**.

4. Click **Save**.

Deleting service categories

You can delete existing service categories.

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

- The service category is not predefined. Whether a service category is predefined, you can see from the description (see Displaying service categories on page 104).
- Service items are no longer assigned to the service category. To remove service items, edit the service category and remove the assigned service items (see Editing service categories on page 106).
- There are no longer child service categories under the service category. To assign child service categories under another service category or to remove them again, edit the corresponding child service category and remove or change the parent service category (see Editing service categories on page 106).

To delete a service category

1. On the menu bar, click **Setup** > **Service categories**.
2. On the **Service Categories** page, in the list, click the service category you want to delete.
3. Click **Delete service category**.
4. In the **Delete Service Category** dialog, confirm the prompt with **OK**.

A

Appendix: Attestation conditions and approval policies from attestation procedures

When attestation policies are created or edited (see Setting up attestation policies on page 56 or Editing attestation policies on page 58), 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.

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	Use the **Lower limit** and **Upper limit** fields to define a risk index

Condition	Description
with defined risk index	range. Attests application roles with a risk index in the chosen range.
Application roles with matching name	Enter part of a name of application roles with access to attest. All application roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.

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

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

Attesting memberships in system entitlements

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

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

Condition	Description
All system entitlements	Attests memberships in all system entitlements.
Specific employees	Select the identities. Attests this identity's memberships (or their associated user accounts) in system entitlements.
Specific employees with subidentities.	Select the identities. Attests this identity's memberships (or their associated user accounts) in system entitlements. In addition, it attests sub identities' memberships (or their associated user accounts) that the select identities are assigned to.
Specific system entitlements	Select the system entitlements. Attests memberships in these system entitlements.
Membership by attestation state	Select an attestation status Attests memberships in system entitlements that match this attestation status. • **Denied memberships**: Attests memberships that have been denied.

Condition	Description
	- **All Memberships**: Attests all memberships. - **New memberships**: Attests memberships that have never been attested.
New or not attested for x days	Specify a number of days. Attests memberships in system entitlements that have not been attested for the defined number of days.
No dynamic groups from Active Roles	Attests memberships in all system entitlements. Dynamic groups are ignored in the process.
System entitlements with specific owners	Select the identities. Attests memberships in system entitlements that are managed by these identities.
System entitlements in a target system container	Select the target system containers. Attests memberships in system entitlements found in these target system containers.
System entitlements in target systems	Select the target systems. Attests memberships in system entitlements assigned to these target systems.
System entitlements with defined risk index	Use the **Lower limit** and **Upper limit** fields to define a risk index range. Attests memberships in system entitlements with a risk index in the chosen range.
System entitlements with owners in departments	Select the departments. Attests memberships in system entitlements that are managed by the identities in these departments.
System entitlements with any owner	Attests user account memberships in system entitlements that only have one owner.
System entitlements with matching name	Enter part of a name of system entitlements with user account memberships to attest. All system entitlements that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
System entitlements by assignment origin	Select how user account memberships in system entitlements must be assigned to enable attestation: - **Directly assigned**: Attests memberships that were assigned directly. - **By request**: Attests memberships in system entitlements that

Condition	Description
	were requested. - **By dynamic roles**: Attests memberships in system entitlements that were assigned through dynamic roles. - **Through roles**: Attests memberships in system entitlements that were assigned through roles.

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

Approval policies	Description
Attestation by selected approvers	Click **Assign**/**Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases.
Attestation by selected approvers with automatic removal of assignments	Click **Assign**/**Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.
Attestation by entitlement owner with automatic removal of assignments	Product owners of system entitlements can be approved through attestation cases. Memberships are deleted if attestation is denied and the configuration fits.
Attestation by employee manager and product owner (with peer group analysis)	The following identities can be approved through attestation cases: - Identity managers who are assigned the system entitlements - Product owners of system entitlements after a peer group analysis (see Attestation by peer group analysis on page 66)
Attestation of group memberships by product owner with automatic removal of memberships	Product owners of system entitlements can be approved through attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

Attesting memberships in application roles

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

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

Condition	Description
All roles	Attests memberships in all applications roles.
Application roles with matching name	Enter part of a name of application roles with primary memberships to attest. All application roles that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
Attesting by attestation status	Select an attestation status Attests memberships in application roles that match this attestation status. You can select the follow status: • **Denied memberships**: Attests memberships that have been denied. • **All Memberships**: Attests all memberships. • **New memberships**: Attests memberships that have never been attested.
Specific employees	Select the identities. Attests identity memberships in application roles.
Specific employees with subidentities.	Select the identities. Attests identity memberships in application roles. In addition, this identity's subidentities memberships in application roles are attested.
Specific roles	Select the application roles. Attests memberships in these application roles. Use 🖧 and ☰ to switch between hierarchical and list view. Multi-select is possible.
New or not attested for x days	Specify a number of days. Attests memberships in application roles that have not been attested for the defined number of days.
Roles by assignment type	Select how memberships in application roles must be assigned to enable attestation: • **Directly assigned**: Attests memberships that were assigned directly. • **By request**: Attests memberships that were requested. • **By delegation**: Attests memberships that were delegated.

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

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

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.

Condition	Description
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: **Per** finds "Person", "Personal", "Perfection" and so on.
User accounts with employees in departments	Select the departments. Attests user accounts with identities assigned to these departments. Use ⇅ and ☰ to switch between hierarchical and list view. Multi-select is possible.
User accounts of employees in child departments	Select the departments. Attests user accounts with identities assigned to these or their child departments. Use ⇅ and ☰ to switch between hierarchical and list view. Multi-select is possible.
User accounts of employees with matching names	Enter part of a name of the identities with user accounts to attest. All identities that have this pattern in their name are included. Example: **Per** finds "Person", "Personal", "Perfection" and so on.
New or not attested for x days	Specify a number of days. Attests user accounts that have not been attested for the defined number of days.
All user accounts not assigned to an identity	Only attests user accounts not assigned to an identity (so-called orphaned user accounts).
Linked user accounts	Attests only user accounts that are assigned these identities.
Target system type	Select the target systems types. Attests user accounts in target system of this target system type.

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

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

Attesting system entitlements

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

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

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

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.

About us

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

Contacting us

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

Technical support resources

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

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

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

Index