Copyright 2019 One Identity LLC.
ALL RIGHTS RESERVED.

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

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

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

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

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

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

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

Legend

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

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

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

One Identity Manager Web Portal User Guide
Updated - August 2019
Version - 8.1.1
## Contents

### Getting Started
- Logging on and off ................................................................. 14
- First login/new account ......................................................... 14
- Logging in ............................................................................... 15
- Logging in with security keys ................................................. 16
- Logging in to the Password Reset Portal .................................. 16
- Logging off ............................................................................. 18

### Navigation and use
- The user interface layout ....................................................... 19
- Start page ............................................................................... 20
- Header .................................................................................... 20
- Menu bar ................................................................................. 21
- Making approval decisions about pending items ..................... 24
- Simple navigation ................................................................. 25
  - Simple commands ................................................................ 25
  - Go to start page .................................................................... 25
  - Simple elements ................................................................... 26
  - Installed controls .................................................................. 26
- Searching ................................................................................ 26
  - Running a search .................................................................. 28
  - Context search ..................................................................... 29
  - Advanced search ................................................................... 29
- White pages ............................................................................. 31
  - Displaying white pages ....................................................... 31
- Sorting ..................................................................................... 32
- Bookmarks .............................................................................. 33
  - Setting bookmarks ............................................................. 33
  - Selecting bookmarks ........................................................... 33
  - Deleting bookmarks ............................................................ 34
- Help ......................................................................................... 34
  - Using the help ...................................................................... 34
Support .......................................................... 35
Community ....................................................... 35
Connection ......................................................... 35
Info ..................................................................... 36
Filter .................................................................. 36
Text filters ......................................................... 37
Number filters .................................................... 37
Object filter ........................................................ 38
Filtering the calendar function .......................... 38
Delete filter .......................................................... 38
Grouping and ungrouping columns .................. 39
Show other columns .......................................... 40
Saving views ....................................................... 40
Deleting saved views .......................................... 40
Custom filter conditions .................................... 41
Creating filters using the wizard ....................... 41
Using control elements ...................................... 45
Displaying technical names of database columns . 45
Displaying filter conditions as SQL expressions ... 46
Exporting views ................................................... 46
Mobile view ......................................................... 47
Heatmaps and statistics in the mobile view .......... 48
Managing password questions ......................... 48
Change password ................................................ 50
Changing contact information ........................... 52
    Editing Active Directory user accounts ........ 53
Changing the language ........................................ 54

Security keys (WebAuthn) ............................... 55
Displaying security keys ..................................... 56
Setting up security keys ..................................... 57
Editing security keys .......................................... 57
Deleting security keys ........................................ 58

Requests ............................................................ 60
My requests ....................................................... 61
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Making requests</td>
<td>62</td>
</tr>
<tr>
<td>Requesting from templates</td>
<td>63</td>
</tr>
<tr>
<td>Requesting through a reference user</td>
<td>64</td>
</tr>
<tr>
<td>Request for other employees</td>
<td>65</td>
</tr>
<tr>
<td>Making requests for subidentities</td>
<td>66</td>
</tr>
<tr>
<td>Requesting privileged access</td>
<td>68</td>
</tr>
<tr>
<td>Request history</td>
<td>69</td>
</tr>
<tr>
<td>Resubmitting a request</td>
<td>70</td>
</tr>
<tr>
<td>Process monitoring</td>
<td>70</td>
</tr>
<tr>
<td>Editing requests</td>
<td>71</td>
</tr>
<tr>
<td>Unsubscribing requests</td>
<td>72</td>
</tr>
<tr>
<td>Canceling requests</td>
<td>72</td>
</tr>
<tr>
<td>Renewing requests</td>
<td>72</td>
</tr>
<tr>
<td>Maintaining templates</td>
<td>73</td>
</tr>
<tr>
<td>Creating and editing templates</td>
<td>74</td>
</tr>
<tr>
<td>Using a reference user's requests</td>
<td>74</td>
</tr>
<tr>
<td>Deleting templates</td>
<td>75</td>
</tr>
<tr>
<td>Sharing templates</td>
<td>75</td>
</tr>
<tr>
<td>Adding information</td>
<td>76</td>
</tr>
<tr>
<td>Shopping cart</td>
<td>76</td>
</tr>
<tr>
<td>Viewing requests</td>
<td>77</td>
</tr>
<tr>
<td>Edit shopping cart</td>
<td>78</td>
</tr>
<tr>
<td>Requesting a Starling 2FA token</td>
<td>79</td>
</tr>
<tr>
<td>Requesting products that require multi-factor authentication</td>
<td>81</td>
</tr>
<tr>
<td>Special requests</td>
<td>82</td>
</tr>
<tr>
<td>Requesting groups</td>
<td>82</td>
</tr>
<tr>
<td>Submitting requests</td>
<td>83</td>
</tr>
<tr>
<td>Setting validity periods</td>
<td>84</td>
</tr>
<tr>
<td>Specifying priorities</td>
<td>84</td>
</tr>
<tr>
<td>Failed requests</td>
<td>85</td>
</tr>
<tr>
<td>My actions</td>
<td>85</td>
</tr>
<tr>
<td>Pending requests</td>
<td>86</td>
</tr>
<tr>
<td>Approving pending requests</td>
<td>87</td>
</tr>
<tr>
<td>Canceling pending requests</td>
<td>88</td>
</tr>
<tr>
<td>Displaying and approving complete requests</td>
<td>89</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Object attestations history</td>
<td>108</td>
</tr>
<tr>
<td>Asking a question</td>
<td>109</td>
</tr>
<tr>
<td>Attestation history</td>
<td>109</td>
</tr>
<tr>
<td>Attestation inquiries</td>
<td>110</td>
</tr>
<tr>
<td>Governance administration</td>
<td>111</td>
</tr>
<tr>
<td>Attestation runs</td>
<td>111</td>
</tr>
<tr>
<td>Sending reminders for all attestation runs</td>
<td>112</td>
</tr>
<tr>
<td>Sending reminders about selected attestation policy runs</td>
<td>113</td>
</tr>
<tr>
<td>Extending an attestation run</td>
<td>113</td>
</tr>
<tr>
<td>Attestation policy settings</td>
<td>114</td>
</tr>
<tr>
<td>Viewing attestation policies</td>
<td>115</td>
</tr>
<tr>
<td>Adding attestation policies</td>
<td>115</td>
</tr>
<tr>
<td>Editing attestation policies</td>
<td>116</td>
</tr>
<tr>
<td>Modifying attestation procedures</td>
<td>117</td>
</tr>
<tr>
<td>Copying attestation policies</td>
<td>118</td>
</tr>
<tr>
<td>Deleting attestation policies</td>
<td>118</td>
</tr>
<tr>
<td>Adding conditions</td>
<td>119</td>
</tr>
<tr>
<td>Editing conditions</td>
<td>120</td>
</tr>
<tr>
<td>Deleting conditions</td>
<td>122</td>
</tr>
<tr>
<td>Objects affected by a condition</td>
<td>122</td>
</tr>
<tr>
<td>Updating object selection</td>
<td>123</td>
</tr>
<tr>
<td>Auditing</td>
<td>123</td>
</tr>
<tr>
<td>Viewing attestation cases</td>
<td>124</td>
</tr>
<tr>
<td>Escalation</td>
<td>124</td>
</tr>
<tr>
<td>Compliance</td>
<td>125</td>
</tr>
<tr>
<td>My actions</td>
<td>126</td>
</tr>
<tr>
<td>Pending rule violations</td>
<td>127</td>
</tr>
<tr>
<td>Approving exception approvals</td>
<td>128</td>
</tr>
<tr>
<td>Resolving rule violations</td>
<td>128</td>
</tr>
<tr>
<td>Rule violation history</td>
<td>130</td>
</tr>
<tr>
<td>Pending policy violations</td>
<td>130</td>
</tr>
<tr>
<td>Policy violations</td>
<td>131</td>
</tr>
<tr>
<td>Auditing</td>
<td>132</td>
</tr>
<tr>
<td>Rule violations</td>
<td>132</td>
</tr>
<tr>
<td>Policy violations</td>
<td>132</td>
</tr>
</tbody>
</table>
Compliance rule violations of application roles ........................................ 194
Attesting application roles ........................................................................ 195
Risk index of application roles .................................................................. 199
Application role history ............................................................................. 201
Role memberships of application role members ......................................... 204
Compliance reports of application roles ...................................................... 205
Resources .................................................................................................... 207
    New resources ......................................................................................... 208
Assignment resources .................................................................................. 209
Multi-request resources ............................................................................... 209
Multi-requestable/unsubscribable resources ................................................ 210
Applications ................................................................................................ 211
    Adding new applications ........................................................................ 211
Devices ......................................................................................................... 212
    Adding new devices ............................................................................... 213
    Editing master data .............................................................................. 215
Adding tags for service items ...................................................................... 217
Task delegation ............................................................................................. 218
Delegation ..................................................................................................... 218
    Adding new delegations ...................................................................... 218
    Deleting delegations ........................................................................... 219
Delegation history ....................................................................................... 220
    Displaying delegation history ........................................................... 221
Ownership .................................................................................................... 222
Assigning owners ......................................................................................... 222
    Assigning owners to devices ............................................................. 223
    Assigning system entitlements owners .............................................. 223
Claim ownership ......................................................................................... 224
Auditing ......................................................................................................... 224
Organizations ............................................................................................... 225
Applications ................................................................................................ 226
Business roles .............................................................................................. 227
Multi-request resources .............................................................................. 228
Multi-requestable/unsubscribable resources ................................................ 229
Employees ................................................................................................... 230
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>254</td>
</tr>
<tr>
<td>Master data</td>
<td>254</td>
</tr>
<tr>
<td>Usage</td>
<td>256</td>
</tr>
<tr>
<td>Displaying reports</td>
<td>256</td>
</tr>
<tr>
<td>Exporting reports</td>
<td>256</td>
</tr>
<tr>
<td><strong>Discovering your statistics on the start page</strong></td>
<td>258</td>
</tr>
<tr>
<td>Statistics</td>
<td>258</td>
</tr>
<tr>
<td>Viewing statistics</td>
<td>259</td>
</tr>
<tr>
<td>Hiding statistics</td>
<td>260</td>
</tr>
<tr>
<td>Viewing source data</td>
<td>260</td>
</tr>
<tr>
<td>Apply filter</td>
<td>260</td>
</tr>
<tr>
<td>Heatmap</td>
<td>261</td>
</tr>
<tr>
<td>Viewing data</td>
<td>262</td>
</tr>
<tr>
<td>Viewing changes for a specific period</td>
<td>262</td>
</tr>
<tr>
<td>Limiting the amount of data</td>
<td>262</td>
</tr>
<tr>
<td>Displaying object details</td>
<td>263</td>
</tr>
<tr>
<td>What statistics are available?</td>
<td>263</td>
</tr>
<tr>
<td>High-risk overview</td>
<td>264</td>
</tr>
<tr>
<td>Compliance</td>
<td>264</td>
</tr>
<tr>
<td>Risk</td>
<td>265</td>
</tr>
<tr>
<td>Policies</td>
<td>266</td>
</tr>
<tr>
<td>Organization</td>
<td>266</td>
</tr>
<tr>
<td>IT shop</td>
<td>267</td>
</tr>
<tr>
<td>Attestations</td>
<td>268</td>
</tr>
<tr>
<td>Target systems</td>
<td>268</td>
</tr>
<tr>
<td><strong>About us</strong></td>
<td>271</td>
</tr>
<tr>
<td>Contacting us</td>
<td>271</td>
</tr>
<tr>
<td>Technical support resources</td>
<td>271</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>272</td>
</tr>
</tbody>
</table>
Getting Started

The Web Portal is part of a web application, which you displayed in a web browser. You can use the Web Portal to request and cancel products, and to renew current requests with limited lifetimes. If you own the necessary entitlements, you are able to approve requests and cancellations, perform attestation, view rule violations, and approve or deny exception approvals. Furthermore, you can change your central password and show statistics.

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

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

Tips for using the Web Portal

- Enable JavaScript in your browser for the Web Portal to work.
- You can configure and extend the Web Portal using the Web Designer.
- 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
  - Firefox (release channel)
  - Chrome (release channel)
  - Safari (current version)
  - Microsoft Edge (release channel)
Detailed information about this topic
- Logging on and off on page 14
- Managing password questions on page 48
- Changing contact information on page 52
- Changing the language on page 54
- Navigation and use on page 18

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.

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

Detailed information about this topic
- First login/new account on page 14
- Logging in on page 15
- Logging in with security keys on page 16
- Logging off on page 18

First login/new account

If you do not already have a user account, you will have to create a new one.

To log onto the system for the first time

1. In the address line of your web browser, enter the Web address (URL) of the Web Portal to open the login page for the Web Portal.

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

2. Click Create new user account on the login page.

3. On the Register a new user view, complete at least the Last name and First name mandatory fields and enter your e-mail address.
In the field next to **Security code**, enter the code displayed.

**TIP:** If you cannot clearly identify the code displayed, click **Generate a different code** to display a new code.

5. Click **Save**.

When the responsible manager has approved your account, you will receive an e-mail containing a link.

6. Open the confirmation email and click the link.

7. On the confirmation page, click **Confirm e-mail address**.

8. Define your password and your password questions (see also, **Change password** on page 50 and **Managing password questions** on page 48).

9. You can then log in using this information.

**Related topics**

- **Logging in** on page 15
- **Change password** on page 50
- **Managing password questions** on page 48

## Logging in

Open the Web Portal in a web browser.

If your system is also configured for two-factor authentication, other steps might be required to log in. For more information about logging in with your **security key**, see **Logging in with security keys** on page 16.

**To log in to the Web Portal**

1. In the address line of your web browser, enter the web address (URL) of the Web Portal.

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

2. Enter your full user name in the **Login name** field on the Web Portal's login page.

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

4. Click **Connect**.

   **TIP:** If you have forgotten your password, click **Forgot your password? Click here**.

   Then you are forwarded to the Password Reset Portal. For more information on this topic, see **Change password** on page 50.
Related topics

- First login/new account on page 14
- Logging in with security keys
- Change password on page 50
- Managing password questions on page 48

Logging in with security keys

If your system is appropriately configured and you own and have set up a security key, you can use it to log in to the Web Portal.

**To log in to the Web Portal with a security key**

1. In the address line of your web browser, enter the web address (URL) of the Web Portal.
   
   **TIP:** By default, the URL is http://<server name>/<application name>/, where <server name> is the name of the server on which the Web Portal is installed.

2. On the Web Portal's log in page, enter your login data.
3. Click Log in.
4. Follow the instructions (for example, plug your security key into your USB socket and then touch the contact).
   
   You will be automatically logged in.

Related topics

- First login/new account on page 14
- Logging in on page 15
- Security keys (WebAuthn) on page 55

Logging in to the Password Reset Portal

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

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

- Use a passcode that you have received from your manager.
- Answer your personal password questions.
- Use your user name and personal password to log in to the Web Portal.
To log in to Password Reset Portal using an access code

1. On the Web Portal’s login page, click Manage your passwords or Forgot your password?. This opens the Password Reset Portal.
   The Password Reset Portal opens.
2. On the Select how you want to authenticate yourself page, select the option I have a passcode next to Authentication method.
3. In the Central user account field, enter your user name.
4. Click Next.
5. On the Enter your passcode page, in the Passcode field, enter your passcode.
6. In the field below Enter the security code, enter the CAPTCHA code displayed.
   TIP: If you cannot clearly identify the CAPTCHA code displayed, click Generate a different code. A new CAPTCHA code is then generated.
7. Click Next.

To log in to Password Reset Portal using your password questions

1. On the Web Portal’s login page, click Manage your passwords or Forgot your password?.
   The Password Reset Portal opens.
2. On the Select how you want to authenticate yourself page, select the option I want to answer my secret password questions next to Authentication method.
3. In the Central user account field, enter your user name.
4. Click Next.
5. On the Answer your password questions page, enter the relevant answers to your password questions in the fields.
6. In the field below Enter the security code, enter the CAPTCHA code displayed.
   TIP: If you cannot clearly identify the CAPTCHA code displayed, click Generate a different code. A new CAPTCHA code is then generated.
7. Click Next.

To log in to Password Reset Portal using your current password

1. On the Web Portal’s login page, click Manage your passwords or Forgot your password?.
   The Password Reset Portal opens.
2. On the Select how you want to authenticate yourself page, select the option I log in with my current password next to Authentication method.
3. In the Central user account field, enter your user name.
4. Click Next.
5. On the **I log in with my current password** page, enter your login information in the fields.

6. In the field below **Enter the security code**, enter the CAPTCHA code displayed.

   | TIP: If you cannot clearly identify the CAPTCHA code displayed, click **Generate a different code**. A new CAPTCHA code is then generated.

7. Click **Next**.

### Related topics
- First login/new account on page 14
- Logging in on page 15
- Logging off on page 18

### Logging off

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

**To log off from Web Portal**

1. Click 📡 | **Log off** in the header.
2. In the **Log Off** dialog, confirm the prompt with **Yes**.
   
   Your logoff was successful.

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

### Navigation and use

You use the Web Portal to view and manage data. Some menu are available in the **header**, on the **start page** as well as in the **menu bar**.

| NOTE: What Web Portal functionality is available to the you, depends on the role model stored in the database. Which groups of employees are supplied with which functionality in the standard installation is explained in the following chapters.

**Detailed information about this topic**

- Start page on page 20
- Header on page 20
- Simple navigation on page 25
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 areas from here.

**Top – Menu bar**

The menu bar is displayed horizontally in the upper part of the screen and provides different menus and submenus. To reach the Start page, click 🏠 Start page.

On the top right-hand side of the screen, select 🗼 Settings to access the My Settings view. This page contains other options that you can use to configure your email notification and report settings.

**Work area**

The work area changes depending on the menu you have called via the navigation.

**Related topics**

- Header on page 20
- Menu bar on page 21
- Start page on page 20
Start page

Once you have logged in successfully, the home page appears. Displayed across the home page, there are tiles of different sizes, which 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 Explore.

Detailed information about this topic

- Header on page 20
- Menu bar on page 21

Header

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

Table 1: Functions in the header

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="search_icon.png" alt="Search" /></td>
<td>Search</td>
</tr>
<tr>
<td>The search helps you to search for various objects. For example, you can quickly and simply search for employees, attestation cases or request procedures. For more information, see Searching on page 26 and Running a search on page 28.</td>
<td></td>
</tr>
<tr>
<td><img src="info_icon.png" alt="Information" /></td>
<td>Information</td>
</tr>
<tr>
<td>Use these menu items to view:</td>
<td></td>
</tr>
<tr>
<td>- Pending requests,</td>
<td></td>
</tr>
<tr>
<td>- Request inquiries,</td>
<td></td>
</tr>
<tr>
<td>- Pending attestations,</td>
<td></td>
</tr>
<tr>
<td>- Attestation inquiries,</td>
<td></td>
</tr>
<tr>
<td>- Pending rule violations,</td>
<td></td>
</tr>
<tr>
<td>- Pending policy violations</td>
<td></td>
</tr>
<tr>
<td>and edit them.</td>
<td></td>
</tr>
<tr>
<td><img src="tip_icon.png" alt="TIP" /></td>
<td>TIP: The moment this icon goes orange (🚀), you have tasks pending.</td>
</tr>
<tr>
<td><img src="my_requests_icon.png" alt="My Requests" /></td>
<td>My Requests</td>
</tr>
<tr>
<td>Use these menu items to:</td>
<td></td>
</tr>
</tbody>
</table>
- **Trigger** new requests,
- **Display and edit** your shopping cart,
- **Renew and cancel** products.

**TIP:** The moment this icon goes orange (.orange), you have requests to edit.

### Personal data

Use these menu items to:
- View your personal data with memberships, responsibilities, and entitlements and to edit setting (for example, your **Password questions**),
- **Display** your company's white pages,
- **Log off**.

### Bookmarks

Show and select your bookmarks here.

This icon is only shown if you have saved bookmarks in the Web Portal.

### Help

This menu includes online help, contact to customer service, community links, information about your connection and the product.

Use **Help** to open the context-sensitive help. The help contains the entire contents of the Web Portal User Guide.

**Connection** opens a dialog with detailed information about your web application connection. The information is divided out on **System users**, **Permissions groups** and **Program functions**.

---

### 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, which are respective subtopics.

**To open a menu**

1. In the menu bar, mouse-over a menu.
   
   The menu expands to show more menu items.

2. Click a menu item.
<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu item</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>My requests</td>
<td>• Start new requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show your request history</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit templates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show your shopping cart</td>
</tr>
<tr>
<td>My actions</td>
<td></td>
<td>• Manage pending requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show the approval history</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manage request inquiries</td>
</tr>
<tr>
<td>Auditing</td>
<td></td>
<td>• Display requests of other staff</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show approvals</td>
</tr>
<tr>
<td>Escalation</td>
<td></td>
<td>• Edit escalate requests</td>
</tr>
<tr>
<td>Attestation</td>
<td>My attestation status</td>
<td>• Display your pending attestation cases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Send reminder emails to attestors</td>
</tr>
<tr>
<td>My actions</td>
<td></td>
<td>• Show and edit pending attestations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show the attestation history</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show attestation inquiries</td>
</tr>
<tr>
<td>Auditing</td>
<td></td>
<td>• Show all attestation cases</td>
</tr>
<tr>
<td>Governance</td>
<td>administration</td>
<td>• Show attestation runs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manage attestation policies</td>
</tr>
<tr>
<td>Escalation</td>
<td></td>
<td>• Show escalated attestations</td>
</tr>
<tr>
<td>Compliance</td>
<td>My actions</td>
<td>• Show and approve pending rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show historical rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and edit pending policy violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show historical policy violations</td>
</tr>
<tr>
<td>Auditing</td>
<td></td>
<td>• Show rule violations</td>
</tr>
<tr>
<td>Governance</td>
<td>Administration</td>
<td>• Show policy violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and edit risk index functions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show critical object overview</td>
</tr>
<tr>
<td>Menu</td>
<td>Menu item</td>
<td>Actions</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rules and rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show company policies and policy violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rules with SAP functions and respective rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rules with SAP functions and respective rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rule violations of staff with critical SAP functions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rules and rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show company policies and policy violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rules with SAP functions and respective rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rules with SAP functions and respective rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rule violations of staff with critical SAP functions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rules and rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show company policies and policy violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rules with SAP functions and respective rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rules with SAP functions and respective rule violations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show compliance rule violations of staff with critical SAP functions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Responsibilities</th>
<th>My responsibilities</th>
<th>• Show and manage the staff you are responsible for</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Show and manage system entitlements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage business roles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage system roles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage departments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage cost centers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage locations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage application roles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage assignment resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage multi-request resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage multi-requestable/unsubscribable resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Show and manage devices</td>
</tr>
</tbody>
</table>

| Delegation | Show, create and delete delegations |
|           | Show delegation history |

| Ownerships | Add ownerships |
|           | Assign owners |

| Auditing | Audit employees |
|          | Audit business roles |
|          | Audit system roles |
Making approval decisions about pending items

Pending items are normally, requests, inquiries or attestations.

One way of finding pending items is by selecting the menu **My actions** via 📣 in the header. Pending positions are shown as menu items that you can select. A number next to a menu item indicates the number of pending items of that type and that your action is required to deal with them. This might mean, for example, that you must grant or deny approval to pending requests.

If there are no pending items to deal with or you have already dealt with them all, the white 📣 symbol is displayed.
To make approval decisions about pending items

1. Click 🕵️‍♂️ in the header.
2. Select the area for making approval decisions about pending items.
3. On the new page, do the following:
   - Approve pending items by clicking on ✅ next to the position.
   - Deny pending items by clicking on ⌂️ next to the position.
4. Click Next:
5. On the Approvals page, click Save.

Simple navigation

Simple commands

Table 3: Overview of simple commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab</td>
<td>Navigate between single elements</td>
</tr>
<tr>
<td>Enter or, if required, Space</td>
<td>Confirm input</td>
</tr>
<tr>
<td>Backspace</td>
<td>Navigate to previous page</td>
</tr>
<tr>
<td>Alt + Left arrow or Alt + Right arrow</td>
<td>Navigate to previous or next page</td>
</tr>
</tbody>
</table>

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

Go to start page

Table 4: Overview of key combinations for navigating

<table>
<thead>
<tr>
<th>Key Combinations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAB</td>
<td>Navigate forward</td>
</tr>
<tr>
<td>Shift + TAB</td>
<td>Navigate backwards</td>
</tr>
<tr>
<td>Enter key</td>
<td>Execute an action</td>
</tr>
<tr>
<td>Search</td>
<td>You can use the tab key to select <strong>Search</strong>. Once the box is selected, the search entry disappears and you can enter a new term in <strong>Search</strong>. Confirm your input with Enter.</td>
</tr>
</tbody>
</table>
Simple elements

Table 5: Overview of the controls used

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button</td>
<td>Use the tab key to navigate to the control and press Enter to execute the action.</td>
</tr>
<tr>
<td>Link</td>
<td>Navigate to the required link with TAB and press Enter to open a new page or dialog.</td>
</tr>
<tr>
<td>Popup</td>
<td>Click Esc to leave the popup window without executing anything. Click Enter to execute. If there is more than one action to execute, navigate with TAB to the desired action and execute with Enter.</td>
</tr>
<tr>
<td>Menu</td>
<td>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.</td>
</tr>
<tr>
<td>Input field</td>
<td>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.</td>
</tr>
<tr>
<td>Tiles</td>
<td>Use the tab key to navigate to the tile and press Enter to display the page’s content.</td>
</tr>
<tr>
<td>Checkbox</td>
<td>Use the tab key to navigate to the required checkbox and press Space to enable the checkbox.</td>
</tr>
<tr>
<td>Option</td>
<td>Use the tab key to navigated to the required list of options. Use the arrow keys to choose between the different options. Use Tab to leave the list of options.</td>
</tr>
</tbody>
</table>

Installed controls

Table 6: Overview of other controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tree view</td>
<td>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.</td>
</tr>
</tbody>
</table>

Searching

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

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 7: Rules with examples for searching**

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Doe</td>
<td>Finds John Doe but not John Donut. Search results must contain all of the separate terms in the query. A logical <strong>AND</strong> is used.</td>
</tr>
<tr>
<td>John OR Doe</td>
<td>Finds Jane Doe and John Donut. Placing <strong>OR</strong> between the search terms, acts as a logical OR operator. The result of this search contain at least one of the two search terms.</td>
</tr>
<tr>
<td>John NOT Doe</td>
<td>Finds John but not John Doe. The results of this search do not contain the term that comes after NOT.</td>
</tr>
<tr>
<td>J*</td>
<td>Finds John and Joanna. The * functions as a wildcard for any number of characters to complete the term.</td>
</tr>
<tr>
<td>Do?</td>
<td>Finds Doe but not Donut. The ? functions as a wildcard for a single character to complete the term.</td>
</tr>
<tr>
<td>&quot;John Doe&quot;</td>
<td>Provides results in which the search terms John and Doe follow one another. Results of this search contain the string in quotes as phrase.</td>
</tr>
<tr>
<td>John Doe~</td>
<td>Finds Jon Does but also other similar results. A tilde ~ after the search term indicates that the search should also find similar results. The means that incorrectly spelled terms can be found as well. You can specify the level of similarity by adding a number between 0 and 1 (with decimal point) after the tilde ~. The higher the number, the more similar the results.</td>
</tr>
</tbody>
</table>

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

Use the **Common | Indexing | IndexNonTokenChars** configuration parameter to specify which delimiters are to be used. The configuration parameter can be extended if certain characters in the search text have linking function.

If the **Common | Indexing | IndexUseLegacyAnalyzer** configuration parameter is enabled, alternative tokenizing is performed also. The alternative method of tokenizing is preferable for long tokens. For example, if the string "Department_01" is a token, the partial string "Department" is considered a token.

The following tokens are named.
### Table 8: Tokens for alternative tokenizing

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

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

### Detailed information about this topic

- [Running a search on page 28](#)
- [Context search on page 29](#)
- [Advanced search on page 29](#)

### Running a search

Search is available at all times in the header.
To run a search

1. In the header, enter the search term in the field next to Search. The Search results view opens, displaying all the results that match your query.

Context search

A context search is context-dependent unlike a regular search, and is available where several entries are listed. For example, Request history normally lists several entries and a context search is available above the list.

To run a context search

1. Enter the search term in the field next to Search.
2. Click Search. Any results matching your query are displayed.

Advanced search

Advanced searching is context-dependent, like the context search, but offers various other additional search settings. The advanced search is often found next to the context search and can be opened via a link. You can use the advanced search in the Request history view, for example.

To run an advanced search

1. Click Advanced search in the view above the list. The following table lists the possible search settings.
2. Enable the relevant checkboxes next to the criteria you would like to use to limit the search.
3. Click Search. Any results matching your query are displayed.

Table 9: Setting options for advanced search

<table>
<thead>
<tr>
<th>Category</th>
<th>Setting</th>
<th>Description</th>
<th>Occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display requests</td>
<td>Requests submitted by you for yourself / Requests submitted by the selected employee for himself</td>
<td>If the option is set.</td>
<td>• Request history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - &lt;selected employee&gt; - view Requests</td>
</tr>
<tr>
<td>Category</td>
<td>Setting</td>
<td>Description</td>
<td>Occurs</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Requests submitted</td>
<td>by you for others / Requests submitted by the selected employee for others</td>
<td>If the option is set.</td>
<td>• Request history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Approval history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - &lt;selected employee&gt; - view Requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - Requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - &lt;selected employee&gt; - View Approvals - view Approvals</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - Approvals</td>
</tr>
<tr>
<td>Requests submitted</td>
<td>by others for you / Requests submitted by others for the selected employee</td>
<td>If the option is set.</td>
<td>• Request history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Approval history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - Requests</td>
</tr>
<tr>
<td>Requests submitted</td>
<td>by other users Submitted requests in the selected employee’s organization</td>
<td>If the option is set.</td>
<td>• Request history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Approval history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - Requests</td>
</tr>
<tr>
<td>Filter by request number</td>
<td>Field for number to search for.</td>
<td>Searches for number entered.</td>
<td>• Request history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Approval history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - Requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - &lt;selected employee&gt; - View Approvals - view Approvals</td>
</tr>
<tr>
<td>Request state</td>
<td>Pending</td>
<td>Searches for all pending requests.</td>
<td>• Request history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Approval history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - Requests</td>
</tr>
<tr>
<td></td>
<td>Approved</td>
<td>Searches for all approved requests.</td>
<td>• Request history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Approval history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Auditing - Requests</td>
</tr>
<tr>
<td></td>
<td>Canceled or denied or dismissed</td>
<td>Searches for canceled or denied or dismissed</td>
<td>• Request history</td>
</tr>
<tr>
<td>Delegations</td>
<td>Valid from</td>
<td>Specifies the start of</td>
<td>• Delegation history</td>
</tr>
<tr>
<td></td>
<td></td>
<td>requests.</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Setting</td>
<td>Description</td>
<td>Occurs</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the time period.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid until</td>
<td>Specifies the end of the time period.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delegator</td>
<td>Selection of delegator.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delegation recipient</td>
<td>Selection of the delegation recipient.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Show never assigned</td>
<td>If the option is set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>assigned delegations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**White pages**

Open the **White pages** page using the ✨ | **White pages** menu item (see Displaying white pages on page 31).

White pages allow you to list all people in the company. You can use them in the Web Portal to look up phone numbers, locations, or other information about employees. The white pages also provide you with a quick overview of an employee details (see To display an employee's details on page 32).

On a **White pages** page, you can gather the following information.

**Table 10: White pages**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display</td>
<td>Shows the full name and in brackets, the user name of the employee.</td>
</tr>
<tr>
<td>Primary location</td>
<td>Shows the employee's primary location.</td>
</tr>
<tr>
<td>Primary department</td>
<td>Shows the employee's primary department.</td>
</tr>
</tbody>
</table>

**Related topics**

- Displaying white pages on page 31

**Displaying white pages**

*To display white pages*

- In the header, click ✨ | **White pages**.
To display an employee's details

1. On the **White pages** page, click on an employee.
   In the detail view on the right-hand side, you will see the information.
2. In the detail view, click **Overview**.
   This opens the employee's overview page. Here you can gather further information about the employee (for example, master data, requests, entitlements and so on).
   For more information, see **Displaying information** on page 145.

Related topics

- **White pages** on page 31
- **Displaying information** on page 145

Sorting

A sort function is available to you for all tables.

To sort a table

1. Click in the column header you want to sort.
   You will see an ▼ icon to the right of the column name.
2. Click again in the column header to sort in ascending or descending alphabetical order.
   This sorts the column as required.
3. Click again in the column header to sort in the opposite order.
   This sorts the column as required.

To sort a table by several columns

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

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

Table 11: Multiple column sorting

<table>
<thead>
<tr>
<th>Handling</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the first column.</td>
<td>Click in the column header.</td>
</tr>
<tr>
<td>Select more columns.</td>
<td>Click in the header whilst holding down the Ctrl key.</td>
</tr>
<tr>
<td>Handling</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sort in the opposite order.</td>
<td>Click again in the header whilst holding down the Ctrl key.</td>
</tr>
<tr>
<td>Cancel the sort order/Resort</td>
<td>Click in the header of any column to apply a new sort order.</td>
</tr>
</tbody>
</table>

**Bookmarks**

You sometimes have the option to set bookmarks in views in the Web Portal. Bookmarks have the advantage that you can use them to navigate straight to a particular part in Web Portal when you log in again.

**TIP:** If you frequently request a particular service item from a service category, for example, you can navigate faster to this service category by setting a bookmark.

**Detailed information about this topic**

- Setting bookmarks on page 33
- Selecting bookmarks on page 33
- Deleting bookmarks on page 34

**Setting bookmarks**

**MOBILE:** This function is not available in the mobile interface.

**To set a bookmark**

- Click ✭ Bookmark this page on the page you would like to bookmark.

The Bookmark this page link changes to Remove bookmark. The bookmark is displayed on the start page and in the header.

**NOTE:** Not every page in the Web Portal can be bookmarked.

**Selecting bookmarks**

**To select a bookmark**

- Perform one of the following tasks:
  - On the start page, click the required bookmark in the Bookmarks tile.
  - In the header row, click
and click the required bookmark.
This navigates to the page you have bookmarked.

Deleting bookmarks

MOBILE: This function is not available in the mobile interface.

To delete a bookmark

1. In the header row, click ⬅️ and then select the required bookmark.
2. Click ⬅️ Remove bookmark.
   The link Remove bookmark changes to Bookmark this page and the bookmark is removed.

Help

You will find the ⬅️ Help menu at the right of the screen in the header. Several menu items are shown when you select this menu.

Detailed information about this topic

- Using the help on page 34
- Support on page 35
- Community on page 35
- Connection on page 35
- Info on page 36

Using the help

You can use the guide as well as online help to answer questions about the Web Portal. Online help is accessible in the web application and other areas.

To call up help in the Web Portal

- In the header, click ⬅️ | Help.
  The One Identity Manager Web Portal User Guide opens as online help.
Support

The support portal is there to give you technical support. There you can find a large number of solutions to different issues.

To open the support portal

- In the header, click | Support.
  The support portal opens.

Community

The One Identity Community offers you a forum where you can exchange information and solutions with other users.

To open the One Identity Community forum

- In the header, click | Community.
  This opens the One Identity Community forum.

Connection

You can to call up information about a database session and view it in Web Portal.

TIP: You cannot change any data in the database.

The data connection details are displayed in a dialog window. You can see information about the web application user, permissions groups and the program function allowed.

Information about the user is shown in the System user view. Here, you will find out more about the authentication type, user ID, which permissions the user has (read and/or write access), whether the user is a dynamic user and how the user was added.

You can view permissions groups with a description about each group listed on the Permissions group view.

A list of program functions with a description is available on the Program functions view.

To open the "Connection" dialog.

1. In the header, click | Connection.
2. In Connection, click the tab corresponding to the type of information that you would like to view in more detail.
Info

The **About** menu shows you, among other things, information about your currently installed version of the Web Portal and the registered names of the product. It is displayed in dialog containing the following views.

- **About**
  Displays the registered trade mark names and the current version of the Web Portal installed.
- **Legal Notices**
  Lists components from third-parties included in the Web Portal. The contact data and the component license might also be given.
- **Contact**
  This shows the contact data for purchasing queries or other questions.

**To open the "About" dialog**

1. In the header, click 📌 and then **Info**.
2. Select the view for the information type you want to view in more detail.

Filter

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

<table>
<thead>
<tr>
<th>NOTE:</th>
<th>The contents of filter dialogs vary depending on context. You can filter by text, numeric values, fixed values, such as gender, &quot;yes&quot; or &quot;no&quot;, dates or objects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOBILE:</td>
<td>This function is only available in the list view of the mobile interface.</td>
</tr>
</tbody>
</table>

**To use filter on a column**

1. Open a menu which shows tables.
2. Click ⚙ on the required column.

Detailed information about this topic

- [Text filters](#) on page 37
- [Number filters](#) on page 37
- [Object filter](#) on page 38
- [Filtering the calendar function](#) on page 38
- [Delete filter](#) on page 39
- Grouping and ungrouping columns on page 39
- Show other columns on page 40
- Saving views on page 40
- Deleting saved views on page 41

**Text filters**

You can find a text filter in Product in Request History.

**To apply filter criteria to text**

1. Enter one or more terms in Filter on....
2. Select one of the following criteria from the text filter's menu.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All words</td>
<td>This displays all search results, which contain the term in the field.</td>
</tr>
<tr>
<td>Starts with</td>
<td>Only results, which start with the given term are displayed.</td>
</tr>
<tr>
<td>Ends with</td>
<td>Only results, which end with the given term are displayed.</td>
</tr>
<tr>
<td>One or more words</td>
<td>Only results containing at least on of the given terms are displayed.</td>
</tr>
</tbody>
</table>

**Number filters**

You can find a number filter, for example, in the Risk index column in High Risk Overview.

**To apply filter criteria to numerics**

1. Enter a value in the field or use the arrow keys to set a number.
2. Select one of the following criteria from the numeric filter's menu.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>greater or equal</td>
<td>Only results with a value the same or higher than the given value are shown.</td>
</tr>
<tr>
<td>less or equal</td>
<td>Only results with a value the same or lower than the given value are shown.</td>
</tr>
<tr>
<td>Filter</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td>Between</td>
<td>Only results with a value the between the given values are shown.</td>
</tr>
</tbody>
</table>

**Object filter**

You can find an object filter, for example, in My Responsibilities | Employees Primary department.

**To apply an object filter**

1. Select **Object filter** in the Filter on ... dialog.
   The results are shown by default in a hierarchical structure. Unselected objects are identified with ✗.
   You can switch to list view using the icon and back again with ✗.
2. Click the required object.
   The selected object is labeled with ☑ and listed under **Selected**.
   
   **NOTE:** To deselect an objects, click the object in the detailed content view.
3. Click **Filter on**.
   The filter is applied. The matching results are displayed in the view.

**Filtering the calendar function**

The "Calendar function" filter is, for example, available in Request History in the column Request date.
**To apply filter criteria to the calendar function**

1. Select one of the following criteria in the context menu next to the field.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>After</td>
<td>Only displays results after this date.</td>
</tr>
<tr>
<td>Before</td>
<td>Only displays results before this date.</td>
</tr>
<tr>
<td>Between</td>
<td>Only displays results between these dates. Another field with calendar icons is displayed with this setting.</td>
</tr>
<tr>
<td>This week</td>
<td>Only displays results with this week's date.</td>
</tr>
<tr>
<td>Last week</td>
<td>Only displays results with last week's date.</td>
</tr>
<tr>
<td>This month</td>
<td>Only displays results with this month's date.</td>
</tr>
<tr>
<td>This year</td>
<td>Only displays results with this year's date.</td>
</tr>
</tbody>
</table>

2. Perform one of the following tasks:
   - Click 📅 and select a date.
   - Enter the date in the field.

3. Click **Filter on**.
   The filter is applied. The matching results are displayed in the view.

**Delete filter**

After setting a filter, you can remove it again manually or it is removed automatically when you change views.

**To delete a filter**

- Perform one of the following tasks:
  - Click ✗ in the filtered column.
  - Click ✗ in the row above the entire table.

**Grouping and ungrouping columns**

Grouping is offered for views with a large number of entries. You can group columns in the **Auditing** view on the **Attestation policy** column, for example.

ℹ️ **MOBILE**: This function is only available in the list view of the mobile interface.
To group by column or ungroup

1. Select the filter in the column you want and click **Group by this column**. The entries are displayed in groups.
2. Open the group with ›. This displays all the entries in the group.
- OR -
3. Delete the filter. This dissolves the group.

Show other columns

You can blend in other columns you want to see in your view.

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

To include other columns in the table

1. Click **View settings | Additional columns**. This opens **Additional columns**.
2. Enable the checkbox next to the column you wish to display.
3. Click **Apply**. Now you can see the selected columns in the table and use them.

Saving views

If you have modified a view and wish to use it at a later stage, for example, you can save the view settings.

**TIP:** The saved view is only available at the location where you saved it.

To save the current view

1. Click **View settings | Save current view**. This opens the **Save current view** dialog.
2. Enter a name for the view in the field.
3. Click **Save**.

**TIP:** You can select and apply the saved view at any time under **View settings**.
Deleting saved views

You can delete saved views in view settings.

**TIP:** The saved view is only available at the location where you saved it.

To delete a saved view

1. Click View settings | Edit list.
   This opens the dialog Edit view settings.
2. Click after the view setting that you want to delete.
   The deleted view setting is removed from the dialog and you cannot select it in the menu anymore.

Custom filter conditions

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

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

The wizard is available in different places in the Web Portal (such as People).

**MOBILE:** This function is not available in the mobile interface.

To open the filter wizard

- Click View settings | Open filter wizard.

Detailed information about this topic

- Creating filters using the wizard on page 41
- Using control elements on page 45
- Displaying technical names of database columns on page 45
- Displaying filter conditions as SQL expressions on page 46

Creating filters using the wizard

To create a filter with the wizard, first select a column, edit the conditions and comparison operators. Once these settings have been configured, you can apply the filter.
To create and apply a filter with the wizard

1. Click **View settings | Open filter wizard**.
2. Select the column for the table in the filter wizard.
   a. Click **At least one entry exists** and specify whether the column should reference or be referenced from other tables.

The following views are available.

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

b. Select the desired column in the **Filter wizard** view.
   This inserts a control for the first condition.
3. Enter the condition and configure the following settings:

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

b. Change the comparison operator.
   
   To change the comparison operator, click the comparison operator "is less than", for example.
   
   The type of comparison operator depends on the column type. The following
Comparison operators are available.

### Table 16: Comparison operators

<table>
<thead>
<tr>
<th>Value type</th>
<th>operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text value</td>
<td>is equal to</td>
<td>Finds the same text value.</td>
</tr>
<tr>
<td></td>
<td>Precedes the word in the alphabet</td>
<td>Finds all results that occur before the entered text in alphabetical order.</td>
</tr>
<tr>
<td></td>
<td>Follows the word in the alphabet</td>
<td>Finds all results that occur after the entered text in alphabetical order.</td>
</tr>
<tr>
<td></td>
<td>Not equal</td>
<td>Finds all results that are not the same as the entered text.</td>
</tr>
<tr>
<td></td>
<td>Is contained in</td>
<td>Finds all results that contain the text value.</td>
</tr>
<tr>
<td></td>
<td>Contains</td>
<td>Finds all results that contain the text value.</td>
</tr>
<tr>
<td></td>
<td>Begins with</td>
<td>Finds all results that begin with the entered text value.</td>
</tr>
<tr>
<td></td>
<td>Ends with</td>
<td>Finds all results that end with the entered text value.</td>
</tr>
<tr>
<td></td>
<td>Is equal or precedes the word in the alphabet</td>
<td>Finds all results that either contain the entered text value or occur before the entered text value in alphabetical order.</td>
</tr>
<tr>
<td></td>
<td>Is equal or follows the word in the alphabet</td>
<td>Finds all results that either contain the entered text value or occur after the entered text value in alphabetical order.</td>
</tr>
<tr>
<td>Numerical value</td>
<td>Is less than</td>
<td>Finds all results that are smaller than the entered numerical value.</td>
</tr>
<tr>
<td></td>
<td>Is greater than</td>
<td>Finds all results that are larger than the entered numerical value.</td>
</tr>
<tr>
<td></td>
<td>is equal to</td>
<td>Finds all results that are the same as the entered numerical value.</td>
</tr>
<tr>
<td></td>
<td>Is less or equal</td>
<td>Finds all results that are less than or equal to the entered numerical value.</td>
</tr>
<tr>
<td></td>
<td>Is greater than or equal</td>
<td>Finds all results that are greater than or equal to the entered numerical value.</td>
</tr>
</tbody>
</table>
The value **false** is selected by default. If you change the value to **true**, data appears that matches the content of this column.

d. To negate the defined condition, click **applies**.
   The condition statement is reversed and the data displayed after filtering, does not match this condition. This setting is not available if the Boolean option can be set.

e. Use the operators and or or when applying multiple conditions.

   **NOTE:** Remove the control by clicking **X**.

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

5. Perform one of the following tasks:
   - Apply the filter by clicking **Apply**.
     This returns you to the original view where a message alerts you to the active filter wizard.
   - Close the wizard with **Close**.

## Using control elements

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

**To expand or collapse controls.**

1. Click **View settings | Open filter wizard**.
2. Perform one of the following tasks:
   - Click **Collapse all** in the **Filter wizard**.
   - Click **Expand all** if the controls are collapsed.

## Displaying technical names of database columns

You can display the technical names of database columns instead of the display names.

**To display technical names of database columns**

1. Click **View settings | Open filter wizard**.
2. Click **Show technical name**.
   This displays all the table and column names that occur in the filter wizard with their technical names.
3. If you would like to view the table and column display names again, click Show display.

**Displaying filter conditions as SQL expressions**

In the expert view you can view and edit filter conditions as SQL expressions.

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

**NOTE:** To open the expert view, you must own the role of administrator, auditor or compliance & security officer.

1. Click View settings | Open filter wizard.
2. Click Expert mode.
   - If you have already created a filter, the filter condition is shown in the SQL editor as an SQL expression.
3. Perform one of the following tasks:
   - Edit the SQL expression in the field.
   - Enter the SQL expression in the field.
4. Click Apply.
   - Applies the filter.

**Exporting views**

You can save a view in PDF or CSV format, or as a website for use as a report. This function is available at different points in your web application. For more information, see Exporting reports on page 256.

**NOTE:** You cannot export more than 100 000 data sets. If there are more data set, only the first 100 000 are exported.

*To export a view*

1. Click View settings | Export this view.
   - This opens the dialog Export this view.
2. Select one of the following options:
   - **Export as PDF:** exports the view as a PDF file.
   - **Export as CSV:** exports the view as a CSV file.
   - **Display as website:** exports the view as a report in HTML format.
3. (Optional) Enable the following checkboxes:
• **All pages**: All pages of the view were exported. If this setting is not enabled, only the current page is exported.

• **Remove header**: Removes the first row of the table. This row contains the column names.

   ![NOTE: This setting is only available if you selected the option Export as CSV in the previous step.]

4. Click **Export**. Exports the view.

## Mobile view

The Web Portal is designed for use with desktops computers and mobile devices. The views are adjusted automatically. In the mobile view, some functions are limited or not at available at all.

### Table 17: Handling options for mobiles

<table>
<thead>
<tr>
<th>Action</th>
<th>Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open menu bar</td>
<td>The menu that you find horizontally under the header in the desktop version is opened on mobile devices as follows:</td>
</tr>
<tr>
<td></td>
<td>1. Press ☰.</td>
</tr>
<tr>
<td></td>
<td>List lists the menus under each other.</td>
</tr>
<tr>
<td></td>
<td>2. Press › next to a menu.</td>
</tr>
<tr>
<td></td>
<td>This displays other menu items.</td>
</tr>
<tr>
<td>Display extended functions/header</td>
<td>You open the functions and settings in the header toolbar (such as search) for mobile devices as follows:</td>
</tr>
<tr>
<td></td>
<td>1. Press ☰.</td>
</tr>
<tr>
<td></td>
<td>Menus are displayed next to each other.</td>
</tr>
<tr>
<td></td>
<td>2. Press on one of the following icons:</td>
</tr>
<tr>
<td></td>
<td>• 📕: Opens search.</td>
</tr>
<tr>
<td></td>
<td>• ☰: Contains the menus My profile, My settings, My processes, Telephone book and Log off.</td>
</tr>
<tr>
<td></td>
<td>• ☐: Opens your shopping cart without requests.</td>
</tr>
<tr>
<td></td>
<td>• ☟: Shows any saved bookmarks.</td>
</tr>
</tbody>
</table>
|                                  | ![NOTE: Replace this text with a description of a feature that is noteworthy.]
|                                  | • ☐: Contains the menus Help, Support, Community, Connection and Info.  |

![ONE IDENTITY](image)
Heatmaps and statistics in the mobile view

The following handling options apply for heatmaps and statistics in the mobile view.

<table>
<thead>
<tr>
<th>Action</th>
<th>Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show tooltip</td>
<td>Tap on the statistic or the diagram.</td>
</tr>
<tr>
<td>Display more details about the statistic/diagram in the dialog</td>
<td>Double-tap on the statistic or the diagram.</td>
</tr>
<tr>
<td>Display a tooltip for a heatmap rectangle</td>
<td>Tap the heatmap's rectangle.</td>
</tr>
<tr>
<td>Zoom in on heatmap</td>
<td>Double-tap on the heatmap.</td>
</tr>
</tbody>
</table>

Managing password questions

If you forget your password, you can change it at any time in the Web Portal. For more information, see Change password on page 50. To do this, you need to set three separate questions that only you can answer.

If your password questions are incorrectly answered, you are locked out. You can reset locked password questions at any time. Depending on how the Web Portal is configured, password questions can be deleted even after they have been used correctly.

NOTE: The reminder to set a password question is shown as a tile on the start page. It is shown there until you have set your password questions.

To create new password questions

1. In the header, click 🗒 | My Profile.
2. On the Overview page, click the Password tile.
3. On the Password questions page, click New question.
4. In the New password question, enter the following:
   - Secret question: Enter your question.
   - Secret answer: Enter your answer to the (above) question.
   - Confirm secret answer: Enter your answer to the question again.
5. Click Apply.
6. On the Password questions page, click Save.
To edit password questions

1. In the header, click 🗒️ | My Profile.
2. On the Overview page, click the Password tile.
3. On the Password questions page, next to the password question that you want to edit, click Edit.
4. In the Password question dialog, enter the following:
   - **Secret question**: Enter your question.
   - **Secret answer**: Enter your answer to the (above) question.
   - **Confirm secret answer**: Enter your answer to the question again.
5. Click Apply.
6. On the Password questions page, click Save.

To delete password questions

1. In the header, click 🗒️ | My Profile.
2. On the Overview page, click the Password tile.
3. On the Password questions page, next to the password question you want to delete, click Edit.
4. In the Password question dialog, click Delete.
5. In the Delete password question dialog, confirm the prompt with Yes.
6. On the Password questions page, click Save.

To unlock password questions

**TIP:** On the Password questions page, locked password questions are labeled with (locked).

1. In the header, click 🗒️ | My Profile.
2. On the Overview page, click the Password tile.
3. On the Password questions page, next to the password question you want to unlock, click Edit.
4. In the Unlock password question dialog, confirm the prompt with Yes.
5. On the Password questions page, click Save.

Related topics

- Change password on page 50
Change password

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

You can change your password(s) in 2 steps:

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

Step 1: Log in to the Password Reset Portal

There are three ways to log in to the Password Reset Portal in order to change your password:

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

To log in to Password Reset Portal using an access code

1. On the Web Portal's login page, click Manage your passwords or Forgot your password?
   The Password Reset Portal opens.
2. On the Select how you want to authenticate yourself page, select the option I have a passcode next to Authentication method.
3. In the Central user account field, enter your user name.
4. Click Next.
5. On the Enter your passcode page, in the Passcode field, enter your passcode.
6. In the field below Enter the security code, enter the CAPTCHA code displayed.
   TIP: If you cannot clearly identify the CAPTCHA code displayed, click Generate a different code. A new CAPTCHA code is then generated.
7. Click Next.
8. Proceed as described under Step 2: Change password on page 51.

To log in to Password Reset Portal using your password questions

1. On the Web Portal's login page, click Manage your passwords or Forgot your password?
   The Password Reset Portal opens.
2. On the Select how you want to authenticate yourself page, select the option I want to answer my secret password questions next to Authentication method.
3. In the **Central user account** field, enter your user name.

4. Click **Next**.

5. On the **Answer your password questions** page, enter the relevant answers to your password questions in the fields.

6. In the field below **Enter the security code**, enter the CAPTCHA code displayed.

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

7. Click **Next**.

8. Proceed as described under **Step 2: Change password** on page 51.

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

1. On the Web Portal’s login page, click **Manage your passwords** or **Forgot your password**?

   The Password Reset Portal opens.

2. On the **Select how you want to authenticate yourself** page, select the option **I log in with my current password** next to **Authentication method**.

3. In the **Central user account** field, enter your user name.

4. Click **Next**.

5. On the **I log in with my current password** page, enter your login information in the fields.

6. In the field below **Enter the security code**, enter the CAPTCHA code displayed.

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

7. Click **Next**.

8. Proceed as described under **Step 2: Change password** on page 51.

**Step 2: Change password**

After you have performed the steps from section **Step 1: Log in to the Password Reset Portal** on page 50, the **Manage My Passwords** page is displayed, and you can now change your central password or the passwords for user accounts to which you have access.

**To change the passwords for your personal user accounts or the passwords of other user accounts**

1. On the **Manage my passwords** page, select the option **I want to reset one or more passwords**.

2. Perform one of the following tasks:
To change the passwords for your personal user accounts, click ▸ next to **Personal accounts**.

To change the passwords of other user accounts, click ▸ next to **Other accounts**

3. Select the check box next to the user accounts for which you want to change the password.
4. Click **Next**.
5. On the **Set a new password** page, enter the password you wish to use in the **New password** field.
   
   **TIP:** Below the field, you can see how secure your new password is. To display your company’s password specifications, click **Password policy**.

6. In the **Repeat the password** field, enter the password again.
7. Click **Next**.
   
   The password is reset for the previously selected user accounts.
8. On the **Success** page, click **Log off**.

**To change the central password**

1. On the **Manage my passwords** page, select the option **I want to reset my central password**.
2. Click **Next**.
3. On the **Set a new password** page, enter the password you wish to use in the **New password** field.

   **TIP:** Below the field, you can see how secure your new password is. To display your company’s password specifications, click **Password policy**.

4. In the **Repeat the password** field, enter the password again.
5. Click **Next**.
   
   The central password is reset.
6. On the **Success** page, click **Log off**.

**Related topics**

- Managing password questions on page 48

**Changing contact information**

You can update your contact information at any time.

**NOTE:** You cannot edit light gray boxes.
To update your contact information  

1. In the header, click My Profile.  
2. Click Contact data.  
   
   **NOTE:** Users with other subidentities in addition to their main identity can use the Identity selection field in the Contact data view to select identities. Changes to their contact data only affects the selected identity. This also applies to creating reports. If you create a report it is generated for the selected identity.  
3. Add or correct the entries in the various fields.  
4. Click Change next to Country.  
   The Country dialog opens.  
5. (Optional) Click the filter to limit your search for the required country.  
6. Click the country you would like from the list.  
   The dialog closes and Contact Data is displayed.  
7. Click next to Picture.  
   This opens Picture.  
8. Click Browse... to find a photo.  
   The selected image and other instruction are displayed in the dialog.  
   
   **NOTE:** If the photo is greater than 10 KB, you will have to crop the image.  
9. (Optional) Hold the mouse over the image until a cross cursor appears, left-click and drag the mouse over the image to select the required area.  
10. (Optional) Crop to selection.  
11. Click Apply.  
   The dialog closes and Contact Data is displayed.  
12. Click Save.  

Editing Active Directory user accounts  

You can edit your Active Directory user accounts at any time once you have logged in to the system and the user data has loaded.  

**NOTE:** This function is only available if Active Roles Module is installed. This module references Active Roles extensions in Active Directory user accounts.
To edit your Active Directory user accounts

1. In the header, click ⌂ | My Profile.
2. Click Active Directory user accounts.
3. Enable the required Active Directory user account, if several are available.
4. Edit the fields or add new ones.
5. Save the changes.

Changing the language

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

To change the language for the Web Portal

1. In the header, click ⌂ | My Profile.
2. On the Overview page, click Contact data.
3. On the Personal data page, click Assign or Change next to the Language field.
4. In the Language dialog, select the language you want to use for in the Web Portal.
5. On the Personal data page, click Assign or Change next to the Language for value formatting field.
6. In the Language for value formatting dialog, 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 format MM/DD/JJJJ (12/24/2020).
7. On the Contact data page, click Save.
   The changes will take effect as soon as you call a new page or refresh the page.

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

   TIP: You can change the language of the current session in the Connection dialog under the 🌐 menu.
Security keys (WebAuthn)

Open Security key page, using 🗝️ | My profile | Security keys (see Displaying security keys on page 56).

One Identity offers you the option to log in, simply and securely, to One Identity Manager web applications with help of (physical) security keys. If your system is configured for it and you own security keys like this, you must use the security key when you enter your password to log in to a web application (for example, to the Web Portal). These security keys support the W3C standard WebAuthn.

| IMPORTANT: The WebAuthn standard is NOT support in Internet Explorer. Therefore, use an other browser if you want to log in to One Identity Manager web application using security keys. |

For more information about how you log in to the Web Portal with the help of security keys, see Logging in with security keys on page 16.

If you lose your security key or you cannot use it for any other reason, you can set up a new one using a passcode in the Password Reset Portal (see Setting up security keys on page 57).

On the Security keys page, view your security keys, set up new security keys, edit security keys and delete security keys.

The following tables provide you with an overview of the different functions on the Security keys page.

**Table 19: Security keys**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered</td>
<td>Shows you the date on which the key was registered.</td>
</tr>
<tr>
<td>Last used</td>
<td>Shows you the date on which the security key was last used.</td>
</tr>
<tr>
<td>Times used</td>
<td>Shows you how often the security key has been used.</td>
</tr>
</tbody>
</table>

**Table 20: Controls**

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Use this button, to edit the respective security key.</td>
</tr>
</tbody>
</table>
### Control | Description
--- | ---
Delete | Use this button to delete the respective security key.
New security key | Use this button to set up a new security key.

#### Related topics
- Logging in with security keys on page 16
- Displaying security keys on page 56
- Setting up security keys on page 57
- Editing security keys on page 57
- Deleting security keys on page 58

#### Displaying security keys
You can display your security keys at any time.

**To display your security keys in the Web Portal**

1. In the header, click 🔄 | My Profile.
2. On the Overview page, click the Security keys tile.
   This opens the Security keys page and shows you your security keys and details.

**To display your security keys in the Password Reset Portal**

1. Log in to the Password Reset Portal (see Logging in to the Password Reset Portal on page 16).
2. On the Manage my passwords page, select the I want to manage my security keys option.
   This will display your security keys and details.

#### Related topics
- Security keys (WebAuthn) on page 55
- Setting up security keys on page 57
- Editing security keys on page 57
- Deleting security keys on page 58
Setting up security keys

You can set up or register new security keys at anytime.

NOTE: To set up a security key, you require a physical key that you can connect to your computer by USB or NFC, for example.

To set up a security key in the Web Portal

1. In the header, click My Profile.
2. On the Overview page, click the Security keys tile.
4. Follow the instructions.
   This sets up the security key. You can edit the security key at anytime on the Security keys page.

To set up a security key in the Password Reset Portal

1. Log in to the Password Reset Portal (see Logging in to the Password Reset Portal on page 16).
   TIP: If you loose your security key or you cannot use it for any other reason, you can set up a new one using a passcode in the Password Reset Portal. To do this, you must ask your manager for a passcode and use it to log in to the Password Reset Portal.
2. On the Manage my passwords page, select the I want to manage my security keys option.
3. Click New security key.
4. Follow the instructions.
   This sets up the security key. You can edit the security key at anytime.

Related topics

- Security keys (WebAuthn) on page 55
- Displaying security keys on page 56
- Editing security keys on page 57
- Deleting security keys on page 58

Editing security keys

You can edit security keys at anytime.
To edit a security key in the Web Portal

1. In the header, click ⌐ | My Profile.
2. On the Overview page, click the Security keys tile.
3. On the Security keys page, under the security keys you want to edit, click Edit.
4. In the Edit security key dialog, in the Display name field, enter a name for the security key.
5. Click Save.

To edit a security key in the Password Reset Portal

1. Log in to the Password Reset Portal (see Logging in to the Password Reset Portal on page 16).
2. On the Manage my passwords page, select the I want to manage my security keys option.
3. Under the security keys you want to edit, click Edit.
4. In the Edit security key dialog, in the Display name field, enter a name for the security key.
5. Click Save.

Related topics

- Security keys (WebAuthn) on page 55
- Displaying security keys on page 56
- Setting up security keys on page 57
- Deleting security keys on page 58

Deleting security keys

If you no longer need your security key or you have lost it, you can delete it at anytime.

NOTE: If you only have one key left, you cannot delete it. You last security key can only be deleted by an employee administrator. For more information about how to delete WebAuthn security keys as an employee administrator, see the One Identity Manager Identity Management Base Module Administration Guide.

To delete a security key in the Web Portal

1. In the header, click ⌐ | My Profile.
2. On the Overview page, click the Security keys tile.
3. On the Security keys page, under the security keys you want to delete,
click **Delete**.

4. In the **Security key** dialog, confirm the prompt with **Yes**.

**To delete a security key in the Password Reset Portal**

1. Log in to the Password Reset Portal (see Logging in to the Password Reset Portal on page 16).
2. On the **Manage my passwords** page, select the **I want to manage my security keys** option.
3. Under the security keys you want to delete, click **Delete**.
4. In the **Security key** dialog, confirm the prompt with **Yes**.

**Related topics**

- Security keys (WebAuthn) on page 55
- Displaying security keys on page 56
- Setting up security keys on page 57
- Editing security keys on page 57
Requests

In the **My Requests** menu, you can run various actions and obtain information. The following tables provide you with an overview of the menu items and actions that can be executed here.

**Table 21: Menu items for "Request"**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu item</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>My requests</td>
<td>🌐 New Request</td>
<td>Select and request products from different service categories.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>📝 Request history</td>
<td>Display any requests triggered in the past.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>🔧 Editing requests</td>
<td>Extend or unsubscribe active requests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>🛡️ Maintaining templates</td>
<td>Edit your own or system request templates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>🛍️ Shopping cart</td>
<td>Display the shopping cart and your save for later list.</td>
</tr>
<tr>
<td>My actions</td>
<td></td>
<td>🔄 Pending requests</td>
<td>Approve pending requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>🌐 Approval History</td>
<td>Display any approved or denied past requests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>🌐 Request inquiries</td>
<td>Display submitted request inquiries within the scope of an approval workflow.</td>
</tr>
<tr>
<td>Auditing</td>
<td></td>
<td>🌐 Request</td>
<td>View all requests made within a specific period.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>🌐 Approval</td>
<td>View all requests where a particular employee was involved in the approval decision.</td>
</tr>
<tr>
<td>Escalation</td>
<td></td>
<td>🌐 Request</td>
<td>Edit escalated requests.</td>
</tr>
</tbody>
</table>
NOTE: You can request a variety of products depending on the entitlements assigned to you.

You can apply the following requests:

- Groups
- Membership in roles
- Access to a file system or SharePoint resource
- Every other resource in your area

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

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

Detailed information about this topic

- My requests on page 61
- My actions on page 85
- Auditing on page 97
- IT Shop escalation on page 99

My requests

In My requests, you can execute various actions to do with the requests you manage.

Detailed information about this topic

- Making requests on page 62
- Request history on page 69
- Editing requests on page 71
- Maintaining templates on page 73
- Shopping cart on page 76
Making requests

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 request for other employees in their name.

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

Table 22: Request status

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>The product was requested and has already been assigned. You cannot make another request at the moment.</td>
</tr>
<tr>
<td>✗</td>
<td>The product was already requested or it is not currently available. It cannot be requested at the moment.</td>
</tr>
<tr>
<td>↓</td>
<td>A pending request already exists for this product. You cannot repeat the request at the moment.</td>
</tr>
<tr>
<td></td>
<td>The product was already assigned to the user.</td>
</tr>
</tbody>
</table>

**NOTE:** The product assignments can be inherited, for example. It is not possible to make another request for this product. If the request is repeated, the status changes to This product has already been requested.

To request products

1. In the toolbar, click **Request | My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. On the **Request** page, do the following:
   - In the **Find a service item** field, enter the name of the required product and click **.**
     - OR -
   - Click the required service category.
   
   The relevant products are displayed.

   **TIP:** If you want to change the selected service categories, click **Change service category** and then click the service category you require.

4. (Optional) If the service category contains subcategories, click the selection list followed by the subcategory.
   
   The products contained in the subcategory are listed.

5. (Optional) To summarize the main and subcategories in a list, enable the option Include child categories.
6. Perform one of the following tasks:
   - Right-click **Add to cart** next to the required product.
   - OR -
   - Enable the checkbox next to the required products and click **Add to cart** below the list.

   **TIP:** If you have selected a product upon which other products are dependent, a dialog opens to allow you to request these products along with the others.

7. (Optional) Perform the following steps on the **My shopping cart** page.
   a. Click a request.
   b. Enter further details on the request in the area to the right.
   c. Click ✉.
   d. Repeat these steps where necessary for other orders.

8. (Optional) On the **My Shopping Cart** page, click **Edit**.
   A dialog for the shopping cart opens. You can enter a comment and other information about your shopping cart. This data applies to all items in the shopping cart. For more information, see **Edit shopping cart**.

9. On the **My Shopping Cart** page, click **Submit**.
10. In the **Submit shopping cart** dialog, click **Yes**.

**Detailed information about this topic**

- Requesting from templates on page 63
- Requesting through a reference user on page 64
- Request for other employees on page 65
- Making requests for subidentities on page 66
- Requesting privileged access on page 68

**Requesting from templates**

You can create requests from your own templates or system templates. This helps simplify proper provisioning for a particular job or function. For example, a template may contain all the products a new employee needs to get started. If you use a template for a request, you are not obliged to request all the products in the template. You only have to select the products you want from the template. For more information, see **Maintaining templates** on page 73.

**To request products using a template**

1. In the toolbar, click **Request | My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. On the **Request** page, on the bottom right, click **Actions | Select a request template**.

4. In the **Choose a template** dialog, next to the required request template, click **Add to cart**.

   ![TIP: If you want to display all of the content of the request templates, click ▶ next to the request template.](image)

5. (Optional) Perform the following steps on the **My Shopping Cart** page.
   a. Click a request.
   b. Enter further details on the request in the area to the right.
   c. Click ![](image)
   d. Repeat these steps where necessary for other orders.

6. (Optional) On the **My Shopping Cart** page, click **Edit**.

   A dialog for the shopping cart opens. You can enter a comment and other information about your shopping cart. This data applies to all items in the shopping cart. For more information, see **Edit shopping cart**.

7. On the **My Shopping Cart** page, click **Submit**.

8. In the **Submit shopping cart** dialog, click **Yes**.

---

**Requesting through a reference user**

Use this option to request products that are currently being requested for a selected employee (reference user).

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

1. In the toolbar, click **Request | My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. On the **Request** page, below right click **Actions | Select a reference user**.
4. In the **Select an employee** dialog, click the listed employee whose requests you would like to reproduce.

   ![NOTE: More information can be added to the list of employees. Click View settings | Additional columns and select the information you require from the dialog.](image)

   A new page lists requests, memberships and entitlements for the selected employee.

5. In the **Requests for <Employee name>** window, enable the products that you would also like to request.
6. Click **Add to cart**.
7. (Optional) Perform the following steps on the **My shopping cart** page.
a. Click a request.
b. Enter further details on the request in the section to the right.
c. Click .
d. Repeat these steps where necessary for other orders.

8. (Optional) On the My Shopping Cart page, click Edit.
A dialog for the shopping cart opens. You can enter a comment and other information about your shopping cart. This data applies to all items in the shopping cart. For more information, see Edit shopping cart.


10. In the Submit shopping cart dialog, click Yes.

Request for other employees

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

NOTE: You can filter the list of recipients. For more information, see Filter on page 36.

TIP: You can also order products for other employees directly from the shopping cart.

To make a request for another recipient

1. In the toolbar, click Request | My Requests.
2. On the My requests page, click Start a new request.
3. On the Request page, click Change next to the Recipient field.
4. In the Recipients dialog, click the employees in the list for which you would like to request products.

NOTE: More information can be added to the list of employees. Click View settings | Additional columns and select the information you require from the dialog.

The selected employees are displayed in a list to the right.

5. Click Close.
6. On the Request page, do the following:
   - Enter the product name in the Find a service item field and click .
   - OR -
   - Click the required service category.

The relevant products are displayed.
7. (Optional) If the service category contains subcategories, click ▼ and then subcategory.
   The products contained in the subcategory are listed.
8. (Optional) To summarize the main and subcategories in a list, enable the option
   **Include child categories**.
9. Perform one of the following tasks:
   - Right-click **Add to cart** next to the required product.
   - OR -
   - Enable the checkbox next to the required products and click **Add to cart** below the list.
   **TIP:** If you have selected a product upon which other products are dependent, a dialog opens to allow you to request these products along with the others.
10. (Optional) Perform the following steps on the **My shopping cart** page.
    a. Click a request.
    b. Enter further details on the request in the area to the right.
    c. Click .
    d. Repeat these steps where necessary for other orders.
11. (Optional) On the **My Shopping Cart** page, click **Edit**.
    A dialog for the shopping cart opens. You can enter a comment and other information about your shopping cart. This data applies to all items in the shopping cart. For more information, see **Edit shopping cart**.
12. On the **My Shopping Cart** page, click **Submit**.
13. In the **Submit shopping cart** dialog, click **Yes**.

**Related topics**
- Requesting from templates on page 63

**Making requests for subidentities**

Requests can be made for subidentities in the same manner as for other recipients. If you are logged in to the Web Portal with your main identity, you can trigger a request for yourself and for your subidentities at the same time. If you are logged in with your subidentity, you can only make requests for the current subidentity.
**To request a subidentity**

1. In the toolbar, click **Request | My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. On the **Request** page, click **Change** next to the **Recipient** field.
4. In the **Recipients** dialog, click the subidentities in the list for which you would like to request products.

   **NOTE:** More information can be added to the list of employees. Click **View settings | Additional columns** and select the information you require from the dialog.

   The selected subidentities are displayed in a list to the right.
5. Click **Close**.
6. On the **Request** page, do the following:
   - Enter the product name in the **Find a service item** field and click 🔍.
     - OR -
   - Click the required service category.

   The relevant products are displayed.

   **NOTE:** Grouped service categories are displayed with ▼ and offer other selection options.

   **TIP:** If you would like to change the selected service category or return to the **Request** view, click ⬆️.
7. (Optional) If the service category contains subcategories, click ▼ and then subcategory.

   The products contained in the subcategory are listed.
8. (Optional) To summarize the main and subcategories in a list, enable the option **Include child categories**.
9. Perform one of the following tasks:
   - Right-click **Add to cart** next to the required product.
     - OR -
   - Enable the checkbox next to the required products and click **Add to cart** below the list.

   **TIP:** If you have selected a product upon which other products are dependent, a dialog opens to allow you to request these products along with the others.
10. (Optional) Perform the following steps on the **My shopping cart** page.
   a. Click a request.
   b. Enter further details on the request in the area to the right.
c. Click Edit.

d. Repeat these steps where necessary for other orders.

11. (Optional) On the My Shopping Cart page, click Edit.
A dialog for the shopping cart opens. You can enter a comment and other information about your shopping cart. This data applies to all items in the shopping cart. For more information, see Edit shopping cart.

12. On the My Shopping Cart page, click Submit.

13. In the Submit shopping cart dialog, click Yes.

Requesting privileged access

You can use the Privileged access requests service category to request privileged access to high-security systems (Privileged Account Management system).

| TIP: | For more information about Privileged Account Management see the One Identity Manager Administration Guide for Privileged Account Governance.

To request privileged access

1. In the menu bar, click Request | My requests.

2. In the My requests view, click Start a new request.

3. In the Request window, next to Recipient click Change.

4. In the Recipient view, click the user for whom you want to request the privileged access.

5. Click Close.

6. In the Request view, click Privileged access requests.

7. On the Request page, select how you want to access the system by selecting the check box for the relevant option:
   - Password release request: Request a temporary password.
   - Remote desktop session request: Request temporary access via a remote desktop connection.
   - SSH session request: Request temporary access via an SSH session.

8. On the bottom right, click Move to shopping cart.

9. In the new dialog, next to PAM user account, click Assign.

10. In the PAM user account dialog, select the PAM user account that you want to use for PAM access.

11. Next to System to access/Asset, click Assign.

12. Depending on the type of access you have selected, perform the following actions:
• Password release request: In the **System to access** window, in the **table** menu, select which access you want to request, either a **PAM directory** or a **PAM Asset** and then click the PAM directory or PAM asset in the list.

• Remote desktop session request/SSH session request: In the **Asset** dialog, click the PAM asset you desire.

13. Click **Assign** next to **Account to access**.

14. In the **Account to access** dialog, select in the **Table** menu, select which access you want to request, either **PAM directory account** or a **PAM Asset account**.

15. In the list, select the system account to which you want to request access.

16. (Optional) In the **Comment** field, enter a comment, for example, to justify why you are requesting this access.

17. In the **Valid from** field, specify the time from which you want the access to be valid, or clear the check box for the access to be valid from the time of this request.

   | **TIP:** You can use the icons next to the date field to easily select the date and time from the calendar or from a list.

18. In **Checkout duration**, enter the number of minutes for which the access is valid.

   | **NOTE:** This duration refers to your entry in the **Valid from** field.

19. Click **Save**.

20. Repeat the steps for all additional users and access types.

As soon as the request is approved, a link is displayed in the detailed view of the request in the request history (**Requests | My requests | Request history**). You can use this link to log in to the Privileged Account Management to receive the login data.

### Request history

The request history provides you with an overview of denied, canceled or unsubscribed requests. You can also resubmit requests here.

**To open the request history**

- Open **Request | My Requests** and click **Request History**.

### Detailed information about this topic

- **Resubmitting a request** on page 70
- **Process monitoring** on page 70
Resubmitting a request

You can resubmit requests in the request history. This can be processed faster than submitting a new request and retains the request history.

To resubmit a request

1. Open Request history and select a request.
   This displays more information in the detailed content view.
2. Click Submit again in the master detail.
3. Enter a reason for resubmitting in the request and click OK.
   The request is added to your shopping cart. For more information, see Edit shopping cart on page 78.

To search in the request history

- Use the extended search.
  For more information, see Searching on page 26.

Process monitoring

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

The following compliance states are shown in the request history.

Table 23: Compliance status in the request history

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Request does not generate rule violations.</td>
</tr>
<tr>
<td>🟡</td>
<td>Request generates rule violations.</td>
</tr>
</tbody>
</table>

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

Table 24: Request status in main view

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✈️</td>
<td>Pending/requested Request is being processed.</td>
</tr>
<tr>
<td>✔️</td>
<td>Assigned The request has been assigned.</td>
</tr>
<tr>
<td>✖️</td>
<td>Denied The request was denied. The reason for denial is a policy or</td>
</tr>
</tbody>
</table>
### Status Description

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>rule violation or the manager did not check the request, whether the request has a limited period.</td>
</tr>
<tr>
<td>🚫 Unsubscribed</td>
<td>The request subscription is canceled. For more information, see <a href="#">Unsubscribing requests</a> on page 72.</td>
</tr>
<tr>
<td>🚫 Aborted</td>
<td>The request is terminated or the system could not execute the request. This occurs if no one was responsible for checking the request or if the validity period expired. The request history is displayed with the reason for aborting.</td>
</tr>
<tr>
<td>✔️ Renewal</td>
<td>The request was renewed. For more information about the selected request is shown on the Information tab. Information is for example, who submitted the renewal and when.</td>
</tr>
</tbody>
</table>

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

**To view the current status of your request**

1. Open Request history and mark the request you want.
2. Select a tab in the detailed content view to view more detailed information.

### Editing requests

Requests can be modified until they are unsubscribed. Requests can also be renewed, denied or canceled.

You can execute these tasks in the menu **Edit Requests** in the Web Portal.

- **NOTE:** You can also cancel requests in the Request History menu.

- **NOTE:** You must configure the settings in the Web Designer in order to send cancellations and renewals in the same way as requests in the cart.

**To open the "Edit Request" menu**

- Select the menu Request | My Requests and click Edit Requests.

**Detailed information about this topic**

- [Unsubscribing requests](#) on page 72
- [Canceling requests](#) on page 72
- [Renewing requests](#) on page 72
Unsubscribing requests

You cannot only cancel (or withdraw) requests, you can also unsubscribe them. The difference being that you can only cancel a request within the request process.

Use the Edit Requests menu to unsubscribe. These requests must have the status "assigned". Requests with the status "Assigned" are also listed in the request history but cannot be unsubscribed there.

You can unsubscribe products for other employees if you are responsible for them.

To unsubscribe products

1. Open Edit requests.
   All requests that have been assigned to you are listed in the Renew or Unsubscribe view.
2. Select the desired request and click Unsubscribe.
   NOTE: Request that cannot be selected here, can only be canceled.
3. Enter an optional data and reason for unsubscribing in the Unsubscribe dialog and click Save.
   NOTE: Use the Show request action to display additional products associated with this request.

Canceling requests

Requests that are not assigned can be canceled but not unsubscribed. You can also cancel requests in the request history.

To cancel a request

1. Select Request | My Requests and click Edit Requests.
2. Mark the request you want cancel in Renew or Unsubscribe.
3. Click Withdraw request in the master detail.
   This opens Withdraw request.
4. Enter a reason for canceling in the Withdraw request dialog and confirm with OK.
   The request remains in the request history.

Renewing requests

Some requests are only valid for a limited period. You can renew limited requests at any time, provided you have the required permissions to do it.
NOTE: You must configure the settings in the Web Designer in order to send cancellations and renewals in the same way as requests in the cart.

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

**To renew a request**

1. Open **Edit requests**.
   Requests that are not in your shopping cart are displayed in **Renew or Unsubscribe**.
   All requests are displayed with and without time limits. Sort the requests by validity to list the limited requests sequentially.
2. Renew a request in the name of another employee.
   For more information, see **Request for other employees** on page 65.
3. Enable the request you want to renew and click **Renew**.
4. Edit the renewal date in the dialog and save the changes.

**Maintaining templates**

This menu shows all templates you have created yourself and system-wide templates (created and published by others). By default, products in a template are hidden. You can expand the template you want and view the products and edit them. For more information, see **Requesting from templates** on page 63.

**Table 25: Templates – status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚫</td>
<td>This template has not been approved yet. A decision about publishing it still pending.</td>
</tr>
<tr>
<td>⚪</td>
<td>The template is marked for public use but was not published yet.</td>
</tr>
<tr>
<td>⚫</td>
<td>The template was published.</td>
</tr>
</tbody>
</table>

**To open the “Maintain Templates” menu**

- Open the menu **Request | My Requests** and click **Maintain Templates**.

**Detailed information about this topic**

- Creating and editing templates on page 74
- Using a reference user’s requests on page 74
Creating and editing templates

You can add templates for requests that you make frequently. Templates are added to your shopping cart.

**To create or edit a request template**

1. Add your request to the shopping cart.
   For more information, see Process monitoring on page 70.
2. Open My Shopping Cart and select Create template from shopping cart.
   
   **NOTE:** The list of requests and options for handling them is only shown when there are requests in the shopping cart.

   In the upper part of Cart templates you can see the contents of the shopping cart. Existing request templates are listed in the middle part.
3. Perform one of the following tasks:
   - Select a request template and click select.
   - Enter a name for the new template in the Name of the new template field.
4. Click Create template.

Using a reference user's requests

You can also create templates from reference users' requests. You can add a reference user's request as a new template or insert an existing template.

**To use a reference user's request as template**

1. Add your request to the shopping cart.
   For more information, see Process monitoring on page 70.
2. Open My Shopping Cart and select By reference user.
   
   **NOTE:** More information can be added to the list of employees. Click View settings | Additional columns and select the information you require from the dialog.
3. Select an employee from the list.
Requests, memberships and entitlements are listed. Depending on which requests this employee has triggered or in which hierarchical roles or company resources memberships exist or similar.

4. Enable the item (multi-select is possible) you want to add to the template and click **Create template**.

The selected item is displayed in **Cart Templates**. Your personal templates are also listed.

5. Perform one of the following tasks:
   - Select a template.
     The reference user's items are assigned to the template.
   - Enter a name for the new template and click **Create template**.
     The selected items are assigned to the new template. The new template is added to your list of personal templates.

### Deleting templates

You can remove templates you do not need anymore, at any time. Or perhaps you only want to delete individual items? Then you can edit your request templates. You can only delete your own personal templates.

**To delete an item or an entire template**

1. Open **Maintain templates**.
2. Perform one of the following tasks:
   - Delete your template by clicking  
     - OR -
   a. Open the request template by clicking  
     The template is displayed with all the items it contains.
   b. Highlight the item you want to delete from the template and click  
3. Confirm the prompt with **OK**.

### Sharing templates

You can share your templates with other users by publishing them.

**To share your template with other users**

1. Open **Maintain templates**.
2. Select your template and open the template details with  
3. Enable the options **Template is available to other employees** and **Template
Template has been approved.

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

4. Click **Save**.

**Adding information**

You can add additional information to your personal request templates.

**To add more information to a request**

1. Open **Maintain templates**.
   
   **Cart Templates** is displayed.
   
   **TIP:** Click ≫ next to the template to expand the contents and view each item.
2. Use ≫ to open the template details.
   
   This opens **Edit template**.
3. Enter the desired information in the fields and enable the options.
4. Click **Save**.

**Shopping cart**

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

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

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

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

One of the following icons is displayed in **Status**.
Table 26: Checking status

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑</td>
<td>Request can be made.</td>
</tr>
</tbody>
</table>
| ⚠ | Request violates a rule but can still be made.  
   This icon can also indicate that a mandatory product is missing. |
| ✗ | Request cannot be made due to missing request permissions.  
   Or the product has already been assigned. |

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

To open the "Shopping Cart" menu

- Open the Request | My Requests menu and click Shopping Cart.

Detailed information about this topic

- Viewing requests on page 77
- Editing requests on page 71
- Requesting a Starling 2FA token on page 79
- Requesting products that require multi-factor authentication on page 81
- Special requests on page 82
- Requesting groups on page 82
- Submitting requests on page 83
- Editing validity periods on page 94
- Specifying priorities on page 84
- Failed requests on page 85

Viewing requests

You can view your requests with all their detailed in the shopping cart. If there is a request in your shopping cart, the 🛒 icon is displayed in the header of My Requests.

Tips: If the shopping cart is empty, you can switch to Request, the request history, or your saved for later list from here.
To view your shopping cart

1. Perform one of the following tasks:
   - Open **Shopping Cart**.
   - Click 🛒 in the header.

2. Perform one of the following tasks:
   - This displays all the individual items in your shopping cart.
   - Open the grouped entry by clicking ➔.
     This expands grouped entries and displays more detail.

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

Edit shopping cart

The **Shopping Cart** menu contains several buttons and options that you can use to edit your requests. The buttons and actions are explained in the following table.

Table 27: Edit options in "Shopping Cart"

<table>
<thead>
<tr>
<th>Icon/Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Input fields</strong>&lt;br&gt;These fields are an aid for adding additional information and editing request properties. This additional data could be, for example, that a request violates a compliance rule under specific conditions. These fields are available amongst others in a dialog after triggering a request. Input fields are provided in the following places:&lt;br&gt;&lt;ul&gt;&lt;li&gt;In the shopping cart&lt;/li&gt;&lt;li&gt;Saved for later&lt;/li&gt;&lt;li&gt;In the request template&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>![Trash Can]</td>
<td>Deletes the request&lt;br&gt;&lt;ul&gt;&lt;li&gt;from the shopping cart&lt;/li&gt;&lt;li&gt;From the saved for later list&lt;/li&gt;&lt;li&gt;From the request template&lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>![Save]</td>
<td>Saves additional information in the request's detailed content view.</td>
</tr>
<tr>
<td><strong>Request for multiple employees</strong></td>
<td>Duplicates requests from the shopping cart for other employees. You will find this action action in the main content view in the <strong>Actions</strong> menu. For more information, see <strong>Request for other employees</strong> on page 65.</td>
</tr>
<tr>
<td><strong>Save for Later</strong></td>
<td>Moves requests from the shopping cart to the saved list. You will find</td>
</tr>
</tbody>
</table>
### Icon/Button Table

- **Icon/Button** | **Action**
  - ![icon](icon.png) | Shows the information in the detailed content view about the request currently marked in the shopping cart. In some cases, this icon is available as an action on the product if a request with dependent products cannot be sent.
  - **Check only** | Verifies the requests in the shopping cart. You will find this function in the context menu in **My Shopping Cart**. After checking, you are informed whether the request can be carried out.
  - **Template from from shopping cart** | Creates a template from the shopping cart for reuse. For another employee, for example.
  - **Delete invalid requests** | Removes requests from the shopping cart that either violate a rule or require other entitlements. You will find this function in the context menu in **My Shopping Cart**.
  - **Delete shopping cart** | Deletes the entire shopping cart contents with one click. You will find this function in the context menu in **My Shopping Cart**.
  - **Edit shopping cart** | To edit the shopping cart. For example, to write a reason for the request.
  - **Check & submit shopping cart** | Checks and sends the shopping cart for processing. You can find this button at the bottom of the **My Shopping Cart** view.

### Requesting a Starling 2FA token

The Starling Two-Factor Authentication is a multi-factor authentication and can be used when requesting products or when approving attestations in the Web Portal. For more detailed information about setting up multi-factor authentication, see the One Identity Manager Authorization and Authentication Guide and the One Identity Manager Web Application Configuration Guide.

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

### Table 28: Data for requesting a Starling 2FA token

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile telephone number</td>
<td>Your mobile phone number is mandatory for multi-factor authentication. You can add this in the <strong>Contact</strong> view under <strong>My</strong></td>
</tr>
<tr>
<td>Data</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>Settings, if it is not already there. For more information, see Changing contact information on page 52.</td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td>Entering the country where you live is mandatory. You can add this in the same way as your mobile phone number, under <strong>My Settings</strong>.</td>
</tr>
<tr>
<td><strong>Default email address</strong></td>
<td>You can also add this in the same way, under <strong>My Settings</strong>.</td>
</tr>
</tbody>
</table>

**To request a Starling 2FA token**

1. In the toolbar, click Request | **My Requests**.
2. On the **My requests** page, click **Start a new request**.
3. Click **Access Lifecycle** on the **Request** page.
4. Click **Add to the cart** next to the product **New Starling 2FA token**.
5. Check the mobile telephone number and country code in the dialog.

   **NOTE:** If you have not yet saved a mobile telephone number to your profile, enter your number in the dialog.

6. Click **OK**.
7. (Optional) Perform the following steps on the **My shopping cart** page.
   a. Click a request.
   b. Enter further details on the request in the area to the right.
   c. Click **Save**.
   d. Repeat these steps where necessary for other orders.
8. (Optional) On the **My Shopping Cart** page, click **Edit**.
   A dialog for the shopping cart opens. You can enter a comment and other information about your shopping cart. This data applies to all items in the shopping cart. For more information, see Edit shopping cart.
9. On the **My Shopping Cart** page, click **Submit**.
10. In the **Submit shopping cart** dialog, click **Yes**.
    The request is forwarded to your manager for approval. Once your manager has granted approval, you will receive a text message on your mobile phone with a link to a multi-factor authentication app.
11. Install the app on your smartphone:
    a. Open the text message and click the link.
    b. Download the multi-factor authentication app to your smartphone.
c. Open the app and enter your country code and the mobile phone number.
d. Confirm the given data and enter your email address.
e. Reconfirm and select whether to use telephone or text message contact.
After successful installation, you will receive a registration code.
You can use the app for generating a security code.

**Related topics**

- Requesting products that require multi-factor authentication on page 81
- Confirming terms of use on page 95
- Approving pending requests on page 87
- Approving my attestations on page 104

**Requesting products that require multi-factor authentication**

Multi-factor authentication can be used for specific security-critical requests. Depending on the configuration, either the requester, the order recipient, or the approver must authenticate themselves using an additional security code. Define which products require this authentication in your service items.

For more detailed information about preparing the IT Shop for multi-factor authentication, see the *One Identity Manager IT Shop Administration Guide*. To use multi-factor authentication, you must have a Starling 2FA token. For more information, see Requesting a Starling 2FA token on page 79.

**To request a product that requires multi-factor authentication**

1. In the toolbar, click Request | My Requests.
2. On the My requests page, click Start a new request.
3. On the Request page, click a service category containing products that require multi-factor authentication.
4. Click Add to cart next to the product requiring multi-factor authentication.
5. (Optional) Perform the following steps on the My shopping cart page.
   a. Click a request.
   b. Enter further details on the request in the area to the right.
   c. Click .
   d. Repeat these steps where necessary for other orders.
A dialog for the shopping cart opens. You can enter a comment and other information about your shopping cart. This data applies to all items in the shopping cart. For more information, see Edit shopping cart.

7. On the My Shopping Cart page, click Submit.
8. In the Submit shopping cart dialog, click Yes.
9. In the Terms of use view, enable I have read and understood the terms of use and click Accept.
10. If the product requires multi-factor authentication, you are prompted to enter a security code. It may take a few minutes for the prompt to be displayed.
   - Click Authenticate with Starling 2FA app.
   - OR -
   - Click Send SMS or Phone call and enter the security code that is generated. Click Next.

Special requests

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

- Adding entitlements on page 169
- Adding memberships on page 159
- Deleting memberships on page 160
- Master data on page 168

Requesting groups

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

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

To make a request for Active Directory groups

1. In the toolbar, click Request | My Requests.
2. On the My requests page, click Start a new request.
3. Click the service category Active Directory groups on the Request page.
4. Enable the checkbox next to the required products and click Add to cart below the list.
5. In the New Active Directory security group dialog, enter a group name in the
**Group name** field.

6. Click **OK**.

   **TIP:** Enter a group name that details the naming, type of group and target container. The approver adds the group based on this information. You get more information about the product when you click the product name.

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

7. Perform the following steps on the **My Shopping Cart** page:
   a. Click a request.
   b. Enter further details on the request in the area to the right.
   c. Click ![Edit](image)
   d. Repeat these steps where necessary for other orders.

8. (Optional) On the **My Shopping Cart** page, click **Edit**.

   A dialog for the shopping cart opens. You can enter a comment and other information about your shopping cart. This data applies to all items in the shopping cart. For more information, see **Edit shopping cart**.

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

10. In the **Submit shopping cart** dialog, click **Yes**.

### Submitting requests

After you have added your requests to the shopping cart, edited and checked them, you can submit your shopping cart.

**To submit your requests**

1. Open **My Shopping Cart**.
2. Ensure you only have requests that you really want to submit in your cart.

   **NOTE:** If the shopping cart consists of requests that you want to execute on a regular basis, you can create a template from the shopping cart. For more information, see **Maintaining templates** on page 73.

3. Highlight the request you want and enter more data in the master detail.

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

4. If you want to enter an additional comment about the shopping cart, click **Edit**.
5. Enter a comment about the shopping cart and click **Save**.
NOTE: you can test the request for a rule violation by selecting Check only in the Actions menu. If a rule violation is found, the request is still being processed and requires further approval from managers.

6. Click Submit.
7. Confirm with Yes.

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

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

Setting validity periods

You can specify a validity period for a request or extend its validity period.

To specify the validity period for a product request

1. Open My Shopping Cart.
2. If you want to edit several requests at the same time, click Edit.
   This opens a dialog for the shopping cart.
3. Enter values to fix the validity period of the requests in Valid from and Valid until.

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

Specifying priorities

You can specify the priority of a request in a similar way to the validity period. There are four priority levels.
To specify the priority of requests

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

1. Run the first two steps as described step-by-step in To specify the request validity period.
2. Enable the Apply to all checkbox in the shopping cart’s dialog and select an entry in the menu.
3. Save the changes.

Failed requests

If your request could not be sent when you executed Submit, you can examine the reason for the failure in your shopping cart. The reasons are marked with the icon you know already, in the Status column. For more information, see Shopping cart on page 76.

To view the reason for a failed request

1. Open Service catalog | Shopping cart and click Submit.
2. Confirm Request cannot be submitted with OK.
   Icons are displayed for the products in your shopping cart in Status, which already indicate which product in your request is causing the problem.
3. Highlight the product with the ⚠ icon in your shopping cart and the note Missing required product.
   Required products are listed in the detailed content view. Required products are dependent products. The action to run or information about how to proceed with each item is displayed respectively. For example, if a required product has already been requested and it can only be requested once, it is not possible to request it again. If the missing required product is still in the request, the action 🔄 is provided.
4. Click 🔍 in the master detail to see information about the product’s whereabouts.
   This information is displayed in a dialog. You can see exactly where your request currently is and who the approver is on the Workflow tab.

My actions

My Actions is a submenu of Request. You can execute various actions, such as approve pending requests or handle request inquiries, depending on which entitlements you have been assigned. These actions can be called up over tiles.
Pending requests

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

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

Table 29: Detailed content view of a pending request

<table>
<thead>
<tr>
<th>Tabs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Displays all information about a request. The information displayed varies and is dependent on the service category from which the request was triggered. The following data can be displayed.</td>
</tr>
<tr>
<td></td>
<td>- Product</td>
</tr>
<tr>
<td></td>
<td>- Recipient</td>
</tr>
<tr>
<td></td>
<td>- Requester</td>
</tr>
<tr>
<td></td>
<td>- Processing status</td>
</tr>
<tr>
<td></td>
<td>- Priority</td>
</tr>
<tr>
<td></td>
<td>- Request date</td>
</tr>
<tr>
<td></td>
<td>- Valid from</td>
</tr>
<tr>
<td></td>
<td>- Valid until</td>
</tr>
<tr>
<td></td>
<td>- Renewed until</td>
</tr>
<tr>
<td></td>
<td>- Reason</td>
</tr>
</tbody>
</table>

You do not have to fill all the properties. None of the information can be edited or clicked on apart from the product, Clicking the product opens a Hyper View overview.

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Displays the life cycle chronologically as from the time of request.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Displays any rule violations for this request.</td>
</tr>
</tbody>
</table>
NOTE: Pending requests that have not been granted approval (whether from an approver or automatically is irrelevant) are displayed with a reason in the Pending requests view. Reasons are only displayed if approval has been denied, to provide the next approver with an overview as an aid to reaching the next decision. If you want to see the entire approval workflow for this request, select the Workflow tab in the detailed content view of the selected request.

To open the "Pending Requests" menu

- Open the menu Request | My Actions and click Pending Requests.

Detailed information about this topic

- Approving pending requests on page 87
- Canceling pending requests on page 88
- Displaying and approving complete requests on page 89
- Approving pending Active Directory group requests on page 89
- Approving assignment of new managers on page 90
- Asking a question on page 91
- Deleting questions on page 91
- Revoking hold-status on page 92
- Rerouting approvals on page 92
- Delegating approvals on page 92
- Adding approvers on page 93
- Changing priority on page 93
- Editing validity periods on page 94
- Adding additional items on page 94
- Confirming terms of use on page 95

Approving pending requests

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

NOTE: You can select a predefined text for all undecided approvals in the Standard reason text box or using the Assign link. Standard reasons are displayed in the approval history and in the case details. For more detailed information about default reasons, see the One Identity Manager IT Shop Administration Guide.
Once you have made an approval decision, the request disappears from your list of pending requests.

To make approval decision about a pending request

1. Open **Pending requests** and mark the request you want in the list of pending requests.
2. Perform one of the following tasks:
   - Approve the request with ✔ and click **Next**.
   - Deny the request with ✗ and click **Next**.

   **NOTE:** In **Approvals**, you can enter a reason for your approval decision for all open requests or select a standard reason. You can also add the desired information explicitly to the selected request using **Enter reason** or under the displayed date in **Valid thru**.
3. Perform one of the following tasks.
   a. In the **Approvals** view, select a reason for your decision and click **Save**.
   b. In the **Approvals** view, select a reason for your decision and click **Save**.

   The approval decision reason supports the audit trail.
4. If the product requires multi-factor authentication, you are prompted to enter a security code. It may take a few minutes for the prompt to be displayed.

   - Click **Authenticate with Starling 2FA app**.
   - OR -
   - Click **Send SMS** or **Phone call** and enter the security code that is generated. Click **Next**.

Detailed information about this topic

- Approval history on page 96
- Pending requests on page 86

Canceling pending requests

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

To cancel a request

1. Open **Pending requests** and mark the request you want in the list of pending requests.
2. Click **Withdraw request** in the master detail.
3. Enter a reason for the withdrawal in the dialog and click **OK**.
Displaying and approving complete requests

While handling pending requests, you can display all the requests and grant or deny approval for them all.

To view a complete request and approve all pending requests

1. Open **Pending requests** and mark the request you require in the list of pending requests.
2. Select **Show entire request** under **more**.
3. Perform one of the following tasks:
   a. Grant or deny approval for pending requests by clicking **Approve all** in **Pending Requests**.
   b. Highlight the request you want in **Pending requests** and click **Add items to this request**.

Detailed information about this topic

- Approval history on page 96
- Pending requests on page 86

Approving pending Active Directory group requests

You can enter additional actions for pending requests of an Active Directory group.

To make an approval decision about a new Active Directory group

1. Open **Pending requests** and mark the request from an Active Directory group.
2. Open the dialog window using **Configure the new group** and enter the additional data for the new group.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of the new Active Directory group.</td>
</tr>
<tr>
<td>Container</td>
<td>Selected container.</td>
</tr>
<tr>
<td>Group type</td>
<td>Selected group type.</td>
</tr>
</tbody>
</table>

3. Save the changes.
4. Perform one of the following tasks:
5. Perform one of the following tasks:
   a. In the Approvals view, select a reason for your decision and click Save.
   b. In the Approvals view, select a reason for your decision and click Save.
      The approval decision reason supports the audit trail.
   c. Enter the request’s expiry date if necessary and click Save.
      
      NOTE: The setting with the expiry date is only available when approving the request.

Detailed information about this topic

- Approval history on page 96
- Pending requests on page 86

Approving assignment of new managers

If a manager wishes to assign a new manager for their employee, they must first select a new manager in the employee's master data and select a deadline for the change-over. This triggers a New manager assignment request. For more information, see Assigning new managers on page 148.

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

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

To make an approval decision about a new manager

1. Open Pending requests and highlight the product New manager assignment in the list of pending requests.

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

2. Open the list of assigned entitlements using the link View user’s entitlements and mark the required entitlement.

3. Perform one of the following tasks:
   - Enable the checkbox Delete on the effective date and click Save.
   - Enable the checkbox Cancel on the effective date and click Save.

4. Perform one of the following tasks:
• Approve the request with ✅ and click Next.
• Deny the request with ❌ and click Next.

The marked request is displayed in Approvals.

5. Perform one of the following tasks:
   • In the Approvals view, select a reason for your decision and click Save.
   • In the Approvals view, select a reason for your decision and click Save.
     The approval decision reason supports the audit trail.
   • Enter the request's expiry date if necessary and click Save.

   ¡NOTE: The setting with the expiry date is only available when approving the request.

Detailed information about this topic

- Approval history on page 96
- Pending requests on page 86

Asking a question

Before you make a decision about an approval you can ask a user a question about this request.

To ask for help

1. Open Pending requests and mark the request you require in the list of pending requests.
2. Select Ask for help from the more menu in the master detail.
3. Perform one of the following tasks:
   • Select an employee from the list in the Submit an inquiry about this request dialog.
   • Use the extended search.
   • Use a filter and then mark the item you want in the result list.
4. Enter your query about the request in Submit an inquiry about this request and click Save.
   A message, saying that the inquiry was sent, is displayed in Pending Requests.

Deleting questions

If your problem has become irrelevant, you can recall your question.
**To delete an inquiry**

1. Select the request that you made the inquiry about and click **Recall last question**.
2. Enter a reason for recalling the inquiry in **Recall last question** and click **OK**.

**Revoking hold-status**

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

**To revoke hold status**

1. Highlight the request you want to take off hold.
2. Click **Revoke hold status** in the master detail.

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

**Rerouting approvals**

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

**To reroute an approval**

1. Open **Pending requests** and mark the request you require in the list of pending requests.
2. Select **Reroute approval** from the more menu in the master detail.
3. Select one of the single approval steps in **Reroute approval** and click **Reroute approval**
4. Enter a reason for rerouting in the field and click **Reroute approval**.

**Delegating approvals**

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

**To delegate an approval**

1. Open **Pending requests** and mark the request you require in the list of pending requests.
2. Select **Delegate approval** from the more menu in the master detail.
This displays **Select an employee who should approve instead.**

3. Perform one of the following tasks:
   a. Select an employee from the list in **Select an employee who should approve instead.**
   b. Use the extended search.
   c. Use a filter and then mark the item you want in the result list.

For more information, see **Navigation and use** on page 18.

4. Enter a reason for the delegation in the dialog and click **Save.**
   A message, saying that the delegation was sent, is displayed in **Pending Requests.**

## Adding approvers

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

**To add more approvers to the request**

1. Open **Pending requests** and mark the request you require in the list of pending requests.
2. Select **Add approver** from the **more** menu in the main detail.
3. Perform one of the following tasks:
   a. Select an employee from the list in **Select additional approvers,**
   b. Use the extended search.
   c. Use a filter and then mark the item you want in the result list.
   d. Click the filter icon in **Display** or another column to limit the search for the employee for your inquiry.

For more information, see **Navigation and use** on page 18.

4. Enter a reason for adding another approver in the dialog and click **Save.**
   A message, saying that the additional approver was entered, is displayed in **Pending Requests.**

## Changing priority

You can view pending requests in the **Pending requests** view. The list can be sorted in ascending or descending order. For more information, see **Sorting** on page 32.

**NOTE:** The **Priority** menu is enabled by default and can be applied. You can disable the **Priority** menu using a configuration parameter in the Web Designer. For detailed information about enabling configuration parameters, see the One Identity Manager Web Designer Object Model Documentation.
As an approver of pending requests, you can edit the priority of certain request to influence their position in the sort order. This means, request with high priority are listed at the top if the list is sorted in descending order.

**To change a request’s priority**

1. In the header, click **Request | My Actions**.
2. On the **My Actions** page, click **Pending requests**.
3. On the **Pending Requests** page, select your request in the list of pending requests.
4. In the detailed content view, click **More | Change priority**.
5. In the **Set the priority for this request** dialog, click the priority you want in the **Priority** menu.
6. Click **Apply**.
7. Then make a approval decision about the request (see **Approving pending requests** on page 87).

   | NOTE: The modified priority is not changed until you have saved your approval decision about the request.

**Editing validity periods**

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

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

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

**To edit a request’s validity period**

1. Open **My Actions | Pending requests** and mark the request you require in the list of pending requests.
2. Select **Change validity period** from the **more** menu in the master detail.
3. Edit **Valid until** in **Set the validity period for this request** and click **Apply**.

**Adding additional items**

You can add additional items to pending request by going to the **Request** menu from here.
To add additional products to a request

1. Open Pending requests and mark the request.
2. Select Show entire request under more.
3. Click Add items to this request in Request overview.
4. Add the products you want to your shopping cart in Request and click Submit.

Confirming terms of use

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

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

1. Open Pending Requests and mark the request for which the confirmation of terms of use by the requester is required.

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

2. Perform one of the following tasks:
   - Approve the request with ✔ and click Next.
   - Deny the request with ✗ and click Next.

   Approvals displays your approvals.

3. Perform one of the following tasks:
   - In the Approvals view, select a reason for your decision and click Save.
   - In the Approvals view, select a reason for your decision and click Save.
       The approval decision reason supports the audit trail.
   - Enter the request's expiry date if necessary and click Save.

4. If the product requires multi-factor authentication, you are prompted to enter a security code. It may take a few minutes for the prompt to be displayed.
   - Click Authenticate with Starling 2FA app.
   - OR -
   - Click Send SMS or Phone call and enter the security code that is generated. Click Next.
Approval history

In the approval history, you can view all products you have assigned, denied or canceled, or still being processed (status "Request"). The menu item Approval History is the same as Request History in its structure and content. For more information, see Process monitoring on page 70.

To open the "Approval History" menu

- Open the menu My Actions and click Approval History.

Detailed information about this topic

- Searching for approvals on page 96
- Withdrawing delegation on page 96
- Withdrawing additional approval on page 97

Searching for approvals

In the approval history, you can search, using the advanced search, for products that were assigned to you for approval.

To use the advanced search function in the approval history

1. Open Approval history.
2. Use the extended search.

For more information, see Searching on page 26.

Withdrawing delegation

You can only withdraw delegations if the product has the status "Request".

To cancel a delegation

1. Open Approval history.
   This shows all the products you have assigned, denied, canceled or edited.
2. Highlight the required request and click Withdraw request in the master view.
3. Click Withdraw delegation in the dialog.

   NOTE: Withdraw delegation is only shown if approval of this product was transferred to someone else.

4. Enter a reason for the withdrawal in the next dialog and click Save.

For more information, see Approving pending requests on page 87.
Withdrawing additional approval

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

To cancel additional approval

1. Open Approval history.
   This shows all the products you have assigned, denied, canceled or edited.
2. Highlight the request you want to withdraw and click Withdraw additional approval in the master detail.

   NOTE: Withdraw additional approver is shown if an additional approver was added to this product.
3. Enter a reason for the withdrawal in the field in the dialog and click Save.

For more information, see Approving pending requests on page 87.

Request inquiries

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

You can query requests or attestation cases. Request Inquiries are displayed in under Request Inquires. You can see more information about the inquiry in the detailed content view. The age is empty if there are not inquiries.

For more information, see Pending requests on page 86.

To answer an approval inquiry

1. Open Request | My tasks and click Request inquiries.
2. Mark an inquiry in Request Inquiries.
3. Click Respond to enter an answer.

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

Auditing

Auditing is a submenu of the Request. You can execute various actions, such as viewing all requests or viewing all approved requests, depending on which entitlements you have been assigned. These actions can be called up over tiles.
Detailed information about this topic

- Request on page 98
- Approvals on page 98

Request

This overview lists all requests that have been created with the selected time period. You can select an employee to view just their requests. To limit the number of list entries you can use the advanced search, the filter function or you can select more columns to display. For more information, see Requests on page 60. Marked requests provide the following information in the detailed content view.

- Details of the requested item
- Status indicates the latest action performed on the request
- General information about the request, including all steps the request has completed, and the next steps
- Details of the recipient and requester
- If there are any rule violations for the request these are displayed with At least one rule was violated.

To view historical requests

1. Open Auditing | Request and select an employee via Assign.
2. Perform one of the following tasks:
   - Use a filter and then mark the item you want in the result list.
   - Use the extended search.
   - Mark the entry you want in the list.

This displays details of the selected item in the detailed content view.

⚠️ NOTE: The Workflow tab in the detailed content view shows all changes chronologically in the form of a workflow diagram. Use to open a dialog and view the requester and request number.

Approvals

You can use the Auditing - Approvals view to see requests involving a particular employee. This view is the same as on Auditing - Requests. Use the search function to search for a particular request or to filter the results.
To display all historical requests for a specific approver

1. Open Auditing | Approvals and select an approver via Assign.
2. Perform one of the following tasks:
   - Use the extended search.
   - Mark the entry you want in the list.
This displays details of the selected item in the detailed content view.

   **NOTE:** The Workflow tab in the detailed content view shows all changes chronologically in the form of a workflow diagram.

IT Shop escalation

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

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

Detailed information about this topic

- Escalated request approvals on page 99
- Canceling escalated requests on page 100

Escalated request approvals

As a fallback approver you can make approval decisions about escalated pending requests.

To make approval decisions about escalated pending requests

1. Open IT Shop Escalation.
2. Use a filter and then mark the item you want in the result list.
3. Perform one of the following tasks:
   a. Approve the request with ✔ and click Next.
   b. Deny the request with ✗ and click Next.
   c. Click Approve all and Next.
   d. Click Deny all and Next.
IMPORTANT: The four-eye principle can be broken for decisions because chief approval team members can make decisions for requests at any time!

4. Perform one of the following tasks:
   a. In the Approvals view, select a reason for your decision and click Save.
   b. In the Approvals view, select a reason for your decision and click Save.
      The approval decision reason supports the audit trail.
   c. Enter the request’s expiry date if necessary and click Save.
      NOTE: The setting for the expiry date is only available when approving the request.

Canceling escalated requests

You can cancel escalated requests in IT Shop Escalation.

To cancel escalated pending requests

1. Open IT Shop Escalation.
2. Use a filter and then mark the item you want in the result list.
3. Click Withdraw request in the master view and enter a reason for the withdrawal in the dialog.
Attestation

Attestations require a manager to verify data to ensure that it is compliant. For example, a manager may need to attest to the Active Directory groups to which each of his employees belong.

In **Attestation**, you can, as a Compliance and Security Officer or attestation manager, for example, edit existing or create new policies.

The following tables provide you with an overview of the menu items and actions that can be executed here.

**Table 31: Menu items for the "Attestation" Menu**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu item</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation</td>
<td>My Attestation Status</td>
<td></td>
<td>View your pending attestation cases and send reminder mails to attestors.</td>
</tr>
<tr>
<td>My actions</td>
<td>Pending Attestations</td>
<td>![Edit]</td>
<td>View all pending attestations you are permitted to approve and make an approval decision.</td>
</tr>
<tr>
<td>Attestation history</td>
<td></td>
<td>![View]</td>
<td>View attestations granted or denied approval.</td>
</tr>
<tr>
<td>Attestation inquiries</td>
<td></td>
<td>![View]</td>
<td>View submitted attestation inquiries within the scope of an approval workflow</td>
</tr>
<tr>
<td>Attestation policies</td>
<td>Attestation runs</td>
<td>![View]</td>
<td>View current and predicted values for pending attestation policy runs. Edit expiry date or send reminder emails to attestors.</td>
</tr>
</tbody>
</table>
### Menu item Action Description

<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu item</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Attestation policy</td>
<td>View and edit existing Attestation Policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>policy settings</td>
<td></td>
</tr>
<tr>
<td>Auditing</td>
<td></td>
<td>View all Attestation</td>
<td>View all Attestation Cases in a selected time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cases</td>
<td>period.</td>
</tr>
</tbody>
</table>

**Detailed information about this topic**

- My attestation status on page 102
- My actions on page 105
- Governance administration on page 111
- Auditing on page 123
- Escalation on page 124

### My attestation status

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

The **My Attestation Status** menu shows:

- Attestation cases to be approved by you
- Pending attestation cases
- Attestation cases that you are involved in

If you are an auditor or manager, you also see attestation cases performed by other employees. As a member of the chief approval team, you make approval decisions about attestation cases and assigned attestation cases to other attestors.

In **My Attestation Status**, you can switch between different views.

- Group memberships
- Objects attestation
- All attestation cases

For each case you can see the current status and the creation date in the detailed content view. You can run the following action or get information.

- See whether the case was approved or denied.
- Obtain detailed information about the selected attestation case from the **Information**, **Workflow**, **Attestation policy** and **History** tabs.
- As attestor, you can view attestors for pending attestation cases.
Send a reminder.
As a chief approver make attestation case approval decisions.

### Detailed information about this topic
- Viewing details on page 103
- Attesting pending attestations on page 103
- Sending reminders on page 104
- Approving my attestations on page 104

### Viewing details
You can display details of objects stored with an Attestation History case.

**NOTE:** Objects details are also available in Pending Attestations, Attestation History and Auditing.

#### To view the object details
1. Mark the attestation case you want to view in My Attestation Status.
2. Click Show details on Information.
3. Select an object in Attested object and click View current state of the object.
   This displays an overview with shapes about the attestation. You can see the risk index and run risk index functions in Risk. For more information about risk indexes, see One Identity Manager Risk Assessment Administration Guide.

### Attesting pending attestations
With My Attestation Status, you can display attestators who still have pending attestation. You can send these attestors reminder emails.

**NOTE:** You can also view attestators with pending attestations over Attestation History and Auditing.

#### To notify an attester about pending attestation cases
1. Open My Attestation Status and click View attestors for pending attestation cases.
2. In the Send a reminder mail dialog, click Send a mail next to the employee you want to notify.
   The email program linked to the Web Designer is displayed and an email template with the attester’s email address is opened.
3. Complete and send the email to the attester.  
The email program is closed.

Sending reminders

You can send a reminder to attestors who are assigned to pending attestation cases.

**NOTE:** You can also send reminders to attestors over the menus **Pending Attestations** and **Auditing**.

**To send a reminder to the attestors**

**NOTE:** Reminders can only be sent to attestors for attestation cases with the status **Pending**.

1. Select an attestation case.
2. Click **Send reminder** and write a message to the attestors in the **Send a reminder email** dialog.
3. Click **OK**.

Approving my attestations

You can make approval decisions about your pending attestations in **My Attestation Status**.

**NOTE:** You can also make approval decisions in **Pending Attestations**.

**To approve pending attestations**

1. Open **My Attestation Status**.
2. In **My Attestation Status**, switch to one of the following tabs:
   - Group memberships
   - Objects attestation
   - All attestation cases
3. In the pending attestations view, select the required case.
4. Perform one of the following tasks:
   - Grant approval by clicking ☑.
   - Deny approval by clicking ❌
5. If required, repeat step 3 and click **Next**.
6. Perform one of the following tasks:
- Enter a reason for your decision in the field.
- Select an available reason in the **Standard reason** field.

**NOTE:** You have the option of selecting a predefined text for all cases still to be approved using the **Standard reason** link. Standard reasons are displayed in the approval history and in the case details. For more detailed information about default reasons, see the One Identity Manager Attestation Administration Guide.

7. Click **Save**.

**NOTE:** If you want to grant or deny approval to the entire list of attestation cases, you can set **Approve all** or **Deny all** before clicking **Save**.

8. If the attestation policy requires multi-factor authentication, you are prompted to enter a security code. It may take a few minutes for the prompt to be displayed.

- Click **Authenticate with Starling 2FA app**.
- OR -
- Click **Send SMS** or **Phone call** and enter the security code that is generated. Click **Next**.

For more detailed information about multi-factor authentication for attestations, see the One Identity Manager Attestation Administration Guide.

For more information, see Requesting a Starling 2FA token on page 79.

---

**My actions**

**My Actions** is a submenu of **Attestation**. You can execute various actions to do with the attestations you manage, depending on which entitlements you have been assigned. These actions can be called up over tiles.

**Detailed information about this topic**

- **Pending attestations** on page 105
- **Attestation history** on page 109
- **Attestation inquiries** on page 110

---

**Pending attestations**

Attestations are a way of verifying that security and compliance measures are being met. For example, having a manager attest to the groups his employees belong to provides accountability if security breaches are found. Attestation policies define what and whom to attest.
Attestation policies are run on a schedule, and generate attestation cases. These appear on My Actions. The amount of time you are give to close an attestation case is configured as part of the attestation policy.

As an attestor, you must be able to verify your attestations. Verifying attestations requires reading reports or manually checking object that are attested. If you are not ready to make a decision, you may be able to:

- Generate a report that provides detailed information about the object which you are attesting
- Request more information, add attestors, or delegate the attestation.

Some functions have already been described in the My Attestation Status menu. You can find all the functions available in this menu listed under "Detailed information about this topic".

To open the "Pending Attestations" menu

- Open Attestation | My Actions and click Pending Attestations.

Detailed information about this topic

- Viewing details on page 103
- Sending reminders on page 104
- Pending attestations on page 105
- Approving my attestations on page 104
- Viewing new attestations on page 106
- Adding approvers on page 107
- Attestations for a specific object type on page 107
- Viewing employees authorized to make approvals on page 108
- Object attestations history on page 108
- Asking a question on page 109

Viewing new attestations

All the attestation policy attestation cases are displayed. It is possible that some of the attestation cases have existed for a while and have been approved several times. New cases have not been granted approval yet but might have been denied approval before. These cases are marked with "Yes" in New.

NOTE: You can add the Not approved before column to your table view by showing additional columns. This provides the same information as in the New column, which is shown in the table by default.
To view new attestation cases

1. Open the Pending Attestations menu and select one of the following actions:
   - Click an object type.
     This displays all the matching attestation policies for this object type.
   - Click View attestation policies.
     All existing attestation policies are displayed.
2. Highlight the new attestation case and view more details about the case in the master detail.

Adding approvers

In Pending Attestations, you can add approvers to attestations.

To add an approver

1. Mark an attestation case in Pending attestations and select the action in Add approver.
2. Select an approver from the dialog and enter a reason.
3. Save your data.

Attestations for a specific object type

You can view attestation cases for a specific object type in the Pending attestations menu.

To view attestation for a specific object type

1. Open Pending Attestations and click an object type.
   This displays all the matching attestation policies for this object type.
   
   \[\text{NOTE:} \] How you proceed, depends on the object type you select.
2. Perform one of the following tasks:
   a. Proceed as follows, if you selected **Cost center**.
      A list of your selected object types appears in the view.
      - Select the required cost center.
        This displays the pending attestations for the selected cost center. The **Object attestation** and All attestation cases views are available.
   b. Proceeds as follows, if you select **Employees** or **Business Roles**.
A list of your selected object types appears in the view.

- Select the object type required for viewing the attestation, such as "employee".

In the **Pending Attestations** view, the **Memberships** and **All attestation cases** views are available.

3. Select the required view.
   This displays a list of attestation for the selected view.

4. Highlight the required attestation to view further details.
   In the detailed content view you see several tabs containing detailed information about attestation.

### Viewing employees authorized to make approvals

In **Pending Attestations**, you can view the employees authorized to make approvals for an attestation case.

**NOTE:** This function is also available in **Auditing**.

**To view employees with approval authorization for an attestation case**

1. Open the **Pending Attestations** menu and select one of the following actions:
   - Click an object type.
     This displays all the matching attestation policies for this object type.
   - Click **View attestation policies**.
     All existing attestation policies are displayed.

2. Mark the desired case.
   This displays details of the selected case in the detailed content view.

3. Select the **Workflow** tab.
   This displays the current authorized approvers and approval authorized employees who have already made approvals.

### Object attestations history

In the **Pending Attestations** menu you can view previous attestations of an object.

**NOTE:** This function is also available in **Auditing**.
To view previous attestation cases for an object

1. Open the Pending Attestations menu and select one of the following actions:
   - Click an object type.
     This displays all the matching attestation policies for this object type.
   - Click View attestation policies.
     All existing attestation policies are displayed.
2. Mark the desired case.
   This displays details of the selected case in the detailed content view.
3. Select the History tab.
   This displays a list of the attestation cases that have already taken place for the
   selected object. You can get more information about each attestation case.

Asking a question

Before you make an approval decision about a pending attestation you can ask a user a question about it.

To ask for help

1. Open Pending Attestations and mark the attestation case you want to query.
2. Select Ask for help.
3. Perform one of the following tasks:
   - Select an employee from the list in the Submit an inquiry about this
     attestation case dialog.
   - Use the extended search.
   - Use a filter and then mark the item you want in the result list.
4. Enter your question about the attestation case in the Submit an inquiry about this
   attestation case dialog and click Save.
5. A message stating that the inquiry has been sent is displayed in Pending
   Attestations.

Attestation history

You will find Attestation History in My Actions. Attestation cases that you have granted
or denied are displayed here. If you are an auditor or manager, you may be able to view
attestations performed by other employees. Some functions have already been described
for the My Attestation Status and Pending Attestations menus. You can find all the
functions available in this menu listed under "Detailed information about this topic".
To view attestation cases

1. Open Attestation History.
2. Select one of the following:
   a. approved
   b. not approved
   c. outstanding
3. Perform one of the following tasks.
   a. Use the extended search.
   b. Use a filter and then mark the item you want in the result list.

   The main view provides detailed information about the selected attestation case on the Information, Workflow, Attestation policy and History tabs.

Detailed information about this topic

- Attesting pending attestations on page 103
- Viewing details on page 103
- Viewing employees authorized to make approvals on page 108
- Object attestations history on page 108

Attestation inquiries

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

You can query requests or attestation cases. Attestation inquiries are displayed in Attestation Inquiries. You can see more information about the inquiry in the detailed content view. If there are no inquiries, the page is empty.

To answer an approval inquiry

1. Open Attestation Inquiries.
2. Mark an inquiry in Attestation Inquiries.
3. Click Respond to enter an answer.
   The answer is sent on saving. Confirmation verification is displayed.
Governance administration

The Governance Administration view is a menu item on the Attestation menu. You can execute various actions to do with the attestation policies you manage, depending on which entitlements you have been assigned. These actions can be called up over tiles.

Managers or others responsible for compliance can use attestation policies to run the following tasks.

- Authorize access
- Set up permissions

Attestations start with attestation policies. You use these policies to specify which objects are designated for attestation and when and how often they are run.

You can get a high level overview of the attestations in your organization in the Attestation dashboard. For more information, see What statistics are available? on page 263.

Detailed information about this topic

- Attestation runs on page 111
- Attestation policy settings on page 114

Attestation runs

You will find the Attestation runs menu on the Governance Administration menu. The following table provides a larger overview of which content you can view in Attestation Policy Runs.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation policy</td>
<td>Shows attestation policies that have already been run.</td>
</tr>
<tr>
<td>Run started</td>
<td>Start date of the attestation run.</td>
</tr>
<tr>
<td>Due date</td>
<td>Date on which the attestation run should end.</td>
</tr>
<tr>
<td>Progress so far</td>
<td>Shows the progress of already generated attestation cases of an attestation policy. Progress is shown in percent (only integer values) and with a colored bar. Progress under 70%, red bar. Progress above 90%, green bar. Progress between 70% and 80%, orange bar.</td>
</tr>
</tbody>
</table>

Once you have selected an attestation policy, you can view other details about it. These details are explained in the following table.
Table 33: Description of the detailed content view

<table>
<thead>
<tr>
<th>Content Module / View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>This content module is on Details. You will find information about the attestation run, expiry date, and progress up to now next to the name of the attestation policy.</td>
</tr>
<tr>
<td>Attestation details</td>
<td>This content module you can view current pending, completed, and delegated attestations. Another value is the total value of all existing attestation cases. There are more details about attestation cases with escalation and about speed of attestations.</td>
</tr>
<tr>
<td>Attestation forecast</td>
<td>Details such as the predicted progress on the due date and predicted end date of the run are part of the attestation forecast. More predictions about estimated delays, when attestation would expire under the currently given conditions. Apart from this, attestation is already graded into categories Good, Mediocre, and Bad.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Information about opened and closed attestation cases and the attestors involved are displayed for the selected attestation run on Attestors. You can send reminders to the Compliance &amp; Security Officer and the attestation policy owner but only if there are still pending attestation cases for this attestation policy. You can also renew the attestation, giving a reason.</td>
</tr>
</tbody>
</table>

Detailed information about this topic

- Sending reminders for all attestation runs on page 112
- Sending reminders about selected attestation policy runs on page 113
- Extending an attestation run on page 113

Sending reminders for all attestation runs

You can send reminders to attestators of all the visible attestation runs in the menu Attestation Policy Runs.

To send a reminder to the attestors

2. Click Remind attestors of ALL visible runs and write a message to the attestors in Send reminder mail.
3. Click OK.
Sending reminders about selected attestation policy runs

In Attestation Policy Runs, can also send a reminder to attesters who are responsible for a selected attestation run. Here you have the option to write to all approvers responsible or to individual approvers.

To send a reminder to the attesters
2. Select one of the following:
   a. Good
   a. Mediocre
   b. Bad
3. Select an attestation policy.
   a. Perform one of the following tasks.
      i. Click Send reminder in the main detail window.
         - OR -
      ii. Open the Attestors tab in the main details window and select one or more approvers.
      iii. Below the listed approvers, click the activated Send reminder option.
4. Write a message to the approvers in the Send a reminder mail dialog and confirm by pressing OK.

Extending an attestation run

You can extend an attestation policy run in Attestation policy runs. It is possible to extend all attestation policy runs.

To extend an attestation policy run
1. Open Attestation Policy Runs and mark an attestation policy run.
2. Click Extend attestation run.
3. Enter a new expiry date in the dialog and a reason for the extension.
4. Click OK to confirm.
Attestation policy settings

In the **Attestation Policy Settings** menu, as an administrator, you can create and edit attestation policies. The following functionality can be edited in attestation policies.

- Setting up a schedule after the attestation case is generated.
- Select an employee to be responsible for granting or denying approval of attestation cases.
- Enable/disable the setting used by the system to automatically close redundant attestation cases.

Apart from editing attestation policies, you can also create conditions and edit them. This function makes it possible for you to view all objects adhering to a certain condition.

You cannot edit all the properties in existing policies. This depends on your access permissions. In the **Attestation Policies Settings** menu, all attestation policies with the following information are displayed over various views.

### Table 34: "Attestation Policy Settings" view

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation policy</td>
<td>Name of the attestation policy.</td>
</tr>
<tr>
<td>Attestation procedure</td>
<td>Name of the attestation procedure.</td>
</tr>
<tr>
<td>compliance framework</td>
<td>Compliance frameworks are used for classifying attestation policies, compliance rules and company policies according to regulatory requirements.</td>
</tr>
<tr>
<td>Calculation schedule</td>
<td>Schedule used to generate new attestation cases.</td>
</tr>
<tr>
<td>Owner</td>
<td>Employee that created the attestation policy.</td>
</tr>
<tr>
<td>Actions</td>
<td>Several actions are available in this column. For example, you can edit, copy or delete.</td>
</tr>
</tbody>
</table>

**NOTE:** Include deactivated policies must be set to view these policies.

**Detailed information about this topic**

- Viewing attestation policies on page 115
- Adding attestation policies on page 115
- Editing attestation policies on page 116
- Modifying attestation procedures on page 117
- Copying attestation policies on page 118
- Deleting attestation policies on page 118
- Adding conditions on page 119
• Editing conditions on page 120
• Deleting conditions on page 122
• Objects affected by a condition on page 122
• Updating object selection on page 123

Viewing attestation policies

NOTE: If a Compliance and Security Officer or an attestation manager has assigned ownership of an attestation policy to you, you can view your policy in Attestation Policy Settings.

To view your own attestation policies
1. Open Attestation Policy Settings.
   NOTE: Of the attestation policies you want to view, you are only shown those with attestation runs. If there are no attestation runs, the attestation policies are not listed.
2. Highlight the required attestation policy.
   More information about the policy is displayed in the detailed content view. For more information, see Attestation policy settings on page 114.
   NOTE: If you have no other permissions, you can only view your attestation policies. You cannot edit them.

Adding attestation policies

In the Attestation Policies Settings menu, you can add new attestation policies.

MOBILE: This function is not available in the mobile interface.

To create a new attestation policy
1. Open Attestation Policy Settings.
2. Click New attestation policy and enter the following master data for the attestation policy.
   NOTE: The attestation procedure you select when you create a new attestation policy is important. The selected attestation procedure determines, amongst other things, the available options when conditions are added. The available options are modified to match the attestation procedure.
### Table 35: General master data for attestation policies

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation policy</td>
<td>Field for entering a unique name for the attestation policy.</td>
</tr>
<tr>
<td>Attestation procedure</td>
<td>Selecting the appropriate attestation procedure using Assign.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Selection of the appropriate approval policies using Assign.</td>
</tr>
<tr>
<td>Calculation schedule</td>
<td>Selection of the appropriate calculation schedules using Assign.</td>
</tr>
<tr>
<td>Time required (days)</td>
<td>Select of the number of days which specifies the deadline for making an attestation procedure approval decision.</td>
</tr>
<tr>
<td>Compliance frameworks</td>
<td>Assignment of an attestation policy to a compliance framework using Assign.</td>
</tr>
<tr>
<td>Deactivated</td>
<td>If this option is set, the new attestation is disabled. This option is not set by default.</td>
</tr>
<tr>
<td>Close obsolete tasks automatically</td>
<td>If this option is set, obsolete cases are automatically closed. This option is set by default.</td>
</tr>
<tr>
<td>Description</td>
<td>Field for entering a additional information and conditions for the attestation policy.</td>
</tr>
</tbody>
</table>

3. Click Create.

### Editing attestation policies

You can edit attestation policies in Attestation Policy Settings. If you enable Include deactivated policies, you can also edit these policies.

**To edit an attestation policy**

1. Open Attestation Policy Settings.
2. Mark the desired attestation policy and click in the Actions column.

1. **NOTE:** The system contains default attestation policies. These policies can only be edited to a limited degree. Until now, only Approval policy, Calculation schedule, Processing time and the option Close obsolete tasks automatically could be edited. If you want to make changes to a default attestation policy, create a copy and edit the copy.

1. **NOTE:** If Close obsolete tasks automatically is set, you cannot hide processed attestation cases which are beyond the deadline.
3. Edit the policy as required in **Master data**.
   For more information, see Adding attestation policies on page 115. You can also add new conditions, and change or delete existing ones. Your permissions determine which data you are permitted to edit. For more information, see Adding conditions on page 119.

4. Click **Save**.

**Modifying attestation procedures**

Before you save data or changes for attestation policies, you can set the link type for selecting the object. Set this in **Attestation procedure** when you add or edit a new attestation policy. The following link types are available.

<table>
<thead>
<tr>
<th>Link Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>All conditions must be fulfilled:</td>
<td>New attestation cases are added for all objects fulfilling all of the conditions the next time the attestation policy is executed. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this link type generates a intersecting set of all the individual conditions of the selected objects.</td>
<td>Example: For the attestation policy of type &quot;Membership in organizations&quot;, there are the condition &quot;Departments with matching names&quot; and &quot;Attestation by attestation status&quot;. If this link type is set, the sum of the results for both conditions is displayed in addition to the results for each condition separately.</td>
</tr>
<tr>
<td>At least one condition must be fulfilled:</td>
<td>New attestation cases are added for all objects fulfilling at least one of the conditions the next time the attestation policy is executed. Use of this link type generates a superset of all the individual conditions of the selected objects.</td>
<td>Several conditions apply to the attestation policy mentioned above. During the attestation case, the superset of attestation objects is displayed as the sum of objects found because this link type requires at least condition to be met.</td>
</tr>
</tbody>
</table>

**To select object link types**

1. Open **Attestation Policy Settings**.
2. Perform one of the following tasks:
   a. Create a new attestation policy.
      For more information, see Adding attestation policies on page 115.
   b. Edit the desired attestation policy.
      For more information, see Editing attestation policies on page 116.
3. Perform one of the following tasks:
   a. Assign an attestation procedure to the attestation policy using **Assign** in **Master data**.
   b. Assign a different attestation procedure to the attestation policy using **Change** in **Master data**.
4. Save the changes.

**Copying attestation policies**

In **Attestation Policy Settings**, you can also copy and edit attestation policies. If you enable **Include deactivated policies**, you can also edit these policies. Copied attestation policies can be deleted again.

**To copy an attestation policy**

1. Open **Attestation Policy Settings**.
2. Mark the desired attestation policy and click **Edit** in the **Actions** column.
   
   :white_point: **NOTE:** The system contains default attestation policies. These policies can only be edited to a limited degree. Until now, only **Approval policy**, **Calculation schedule**, **Processing time** and the option **Close obsolete tasks automatically** could be edited. If you want to make changes to a default attestation policy, create a copy and edit the copy.

   :white_point: **NOTE:** If **Close obsolete tasks automatically** is set, you cannot hide processed attestation cases which are beyond the deadline.
3. Edit the policy as required in **Master data**.
   
   For more information, see **Adding attestation policies** on page 115. You can also add new conditions, and change or delete existing ones. Your permissions determine which data you are permitted to edit. For more information, see **Adding conditions** on page 119.
4. Click **Save**.

**Deleting attestation policies**

In **Attestation Policy Settings** you can delete attestation policies. Copied attestation policies can be deleted again both in **Attestation Policy Settings** and **Edit attestation policy**.
To delete an attestation policy

1. Open Attestation Policy Settings.
2. Perform one of the following tasks.
   a. Select the copied attestation policy and click in the Actions column.
   - OR -
   b. Select the required attestation policy that you want to copy or that you have already copied, and click in the Actions column.
   The Edit attestation policy view is displayed.
   c. Click Delete if you no longer need to edit the policy.
3. Confirm the delete prompt with Yes.
The attestation policy is removed from the list.

Adding conditions

When you edit attestation policies, you can also add new conditions to them. You can only add conditions to copies of attestation policies.

To add a condition to a policy

1. Open Attestation Policy Settings.
2. Edit the desired attestation policy.
   For more information, see Editing attestation policies on page 116.
3. In the Master data view, click the Object selection section.
4. Select the required option in the Condition type menu in Edit condition.

   NOTE: The options available in Condition type depend on which attestation procedure is set for the attestation policy to be edited.

The following options are available.

Table 37: Available condition types

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All roles / cost centers</td>
<td>Lists all company structures. Multi-select is possible. Selected parameters are listed in the master detail and can be canceled there. Or you cancel the selection in list again.</td>
</tr>
<tr>
<td>Attestation by attestation status/Roles by assignment type</td>
<td>Lists attestations by status or role assignment type as other parameter. Multi-select is possible. Selected parameters are listed in</td>
</tr>
<tr>
<td>Condition Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Specific roles / cost centers</td>
<td>List certain roles for the company structure, you can toggle between tree view and list view using and . Multi-select is possible. Selected roles are listed in the detailed content view and can be reselected there. Or you cancel the selection in list again.</td>
</tr>
<tr>
<td>Business roles / Application roles / Cost centers with matching names</td>
<td>Displays the Identifier field. Enter a name for the company structure.</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Displays the Count menu. You can enter the count.</td>
</tr>
<tr>
<td>Roles with specific owners / user accounts with specific people / Roles with any owner</td>
<td>Lists certain employees for the company structure. Additional columns can be shown and the filter function applied. Multi-select is possible. Selected employees are listed in the master detail and can be canceled there. Or you cancel the selection in list again.</td>
</tr>
<tr>
<td>Roles with specific role classes</td>
<td>Lists specific role classes. Multi-select is possible. Selected role classes are listed in the master detail and can be canceled there. Or you cancel the selection in list again.</td>
</tr>
<tr>
<td>Roles with defined risk index</td>
<td>Display a scale of 0 to 1 for the risk index and two slide rulers. Specify a beginning and an end value within the scale.</td>
</tr>
<tr>
<td>Roles with owners in departments</td>
<td>Lists departments which have owners. Multi-select is possible. Selected role classes are listed in the master detail and can be canceled there. Or you cancel the selection in list again.</td>
</tr>
</tbody>
</table>

5. Save the changes.

**Editing conditions**

You can rework existing conditions by editing copied attestation policies.
**To add a condition to a policy**

1. Open **Attestation Policy Settings**.
2. Edit the desired attestation policy.
   For more information, see **Editing attestation policies** on page 116.
3. In the **Master data** view, click the **Object selection** section.
4. Select the required option in the **Condition type** menu in **Edit condition**.

   **NOTE:** The options available in **Condition type** depend on which attestation procedure is set for the attestation policy to be edited.

The following options are available.

**Table 38: Available condition types**

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All roles / cost centers</td>
<td>Lists all company structures. Multi-select is possible. Selected parameters are listed in the master detail and can be canceled there. Or you cancel the selection in list again.</td>
</tr>
<tr>
<td>Attestation by attestation status/Roles by assignment type</td>
<td>Lists attestations by status or role assignment type as other parameter. Multi-select is possible. Selected parameters are listed in the master detail and can be canceled there. Or you cancel the selection in list again.</td>
</tr>
<tr>
<td>Specific roles / cost centers</td>
<td>List certain roles for the company structure, You can toggle between tree view and list view using and . Multi-select is possible. Selected roles are listed in the detailed content view and can be reselected there. Or you cancel the selection in list again.</td>
</tr>
<tr>
<td>Business roles / Application roles / Cost centers with matching names</td>
<td>Displays the <strong>Identifier</strong> field. Enter a name for the company structure.</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Displays the <strong>Count</strong> menu. You can enter the count.</td>
</tr>
<tr>
<td>Roles with specific owners / user accounts with specific people / Roles with any owner</td>
<td>Displays the <strong>Count</strong> menu. You can enter the count. Lists certain employees for the company structure. Additional columns can be shown and the filter function applied. Multi-select is possible. Selected employees are listed in the master detail and can be canceled there. Or you cancel the selection in list again.</td>
</tr>
<tr>
<td>Condition Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Roles with specific role classes</td>
<td>Lists specific role classes. Multi-select is possible. Selected role classes are listed in the master detail and can be canceled there. Or you cancel the selection in list again.</td>
</tr>
<tr>
<td>Roles with defined risk index</td>
<td>Display a scale of 0 to 1 for the risk index and two slide rulers. Specify a beginning and an end value within the scale.</td>
</tr>
<tr>
<td>Roles with owners in departments</td>
<td>Lists departments which have owners. Multi-select is possible. Selected role classes are listed in the master detail and can be canceled there. Or you cancel the selection in list again.</td>
</tr>
</tbody>
</table>

**Deleting conditions**

You can delete conditions in **Attestation Policies**. The same applies here as for adding conditions. You can only delete conditions in a copied attestation policy.

*To remove a condition from a policy*

1. Open **Attestation Policy Settings**.
2. Edit the desired attestation policy.
   - For more information, see **Editing attestation policies** on page 116.
3. Highlight the required condition in the Master data view and click the **Actions** column in the **Object selection** section.
   - This deletes the condition.

**Objects affected by a condition**

You can display objects that apply for a specific or all conditions in the **Edit attestation policy** view.

*To allow affected objects to be displayed*

1. Open **Attestation Policy Settings**.
2. Edit the desired attestation policy.
   - For more information, see **Editing attestation policies** on page 116.
3. Perform one of the following tasks:
a. Highlight the required condition and click the linked number in the **Objects** column in the lower area of **Object selection** in the **Master data** view.

b. Click the linked number under the list of conditions.

Any objects that meet the condition(s) are displayed in a dialog.

## Updating object selection

You can update the object selection in **Edit attestation policy** to see modifications. This might be necessary for checking if you have added any new conditions, for example.

### To update the object selection list

1. Open **Attestation Policy Settings**.
2. Edit the desired attestation policy.
   
   For more information, see **Editing attestation policies** on page 116.
3. In the **Master data** view, click the **Object selection** section.

   This reloads the object selection. New conditions, which may also be added to the Manager are also shown. For more information, see the One Identity Manager Attestation Administration Guide.

## Auditing

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

**Auditing** is a submenu of **Attestation** and displays all attestation cases within a selected time period. The content and type of view vary in presentation depending on the respective company.

Some functions have already been described in the **My Attestation Status** menu. You can find all the functions available in this menu listed under "Detailed information about this topic".

### Detailed information about this topic

- Viewing attestation cases on page 124
- Viewing details on page 103
- Sending reminders on page 104
- Viewing employees authorized to make approvals on page 108
- Object attestations history on page 108
- Attesting pending attestations on page 103
Viewing attestation cases

You can gather comprehensive information about attestation cases in the Auditing menu.

To view information about an attestation case

1. Open Auditing and select an employee via Assign.
2. Select one of the following:
   - approved
   - not approved
   - outstanding
3. Perform one of the following tasks:
   - Use a filter and then mark the item you want in the result list.
   - Mark the entry you want in the list.
     This displays details of the selected item in the detailed content view.

Escalation

You will find the Escalation menu on the Attestation menu.

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

NOTE: You only see Escalation if you are a fallback approver or member of the chief approval team.

To view escalated attestations

- Open Escalation.
  This displays escalated attestations.

Escalated attestations are handled in the same way as pending attestations. For more information, see Viewing attestation cases on page 124.

IMPORTANT: The four-eyes principle can be broken for attestations because chief approval team members can make approval decisions about attestation cases at any time!
Compliance

In the **Compliance** menu, you can execute various actions and obtain information. The following tables provide you with an overview of the menu items and actions that can be executed here.

**Table 39: Items in the "Compliance" Menu**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu item</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>My actions</td>
<td>Pending Rule Violations</td>
<td>View all pending rule violations that you are responsible for and can approve.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rule Violation History</td>
<td>View granted exception approvals.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pending Policy Violations</td>
<td>View all pending policy violations that you are responsible for and can approve.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy violations</td>
<td>View edited policy violations.</td>
</tr>
<tr>
<td>Auditing</td>
<td></td>
<td>Rule violations</td>
<td>View all rule violations in the select time period.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy violations</td>
<td>View all policy violations in the select time period.</td>
</tr>
<tr>
<td>Governance administration</td>
<td>High-risk overview</td>
<td></td>
<td>View the top 10 statistics with critical objects, grouped by section. View all critical objects from different sections.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Compliance frameworks</td>
<td>View details about compliance frameworks.</td>
</tr>
<tr>
<td>Menu item</td>
<td>Action</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Rule violations</td>
<td>View all rules</td>
<td>View all rules and their violations that are assigned to Frameworks under</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and their violations</td>
<td>supervision.</td>
<td></td>
</tr>
<tr>
<td>Policy violations</td>
<td>View all policies</td>
<td>View all policies and their violations that are assigned to Frameworks under</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and their violations</td>
<td>supervision.</td>
<td></td>
</tr>
<tr>
<td>Rule analysis</td>
<td>View compliance</td>
<td>View compliance rules containing SAP functions. View SAP user account that</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rules</td>
<td>are involved with the rule violations.</td>
<td></td>
</tr>
<tr>
<td>Function analysis</td>
<td>View compliance</td>
<td>View compliance rule violations by user accounts that are assigned to critical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rules</td>
<td>SAP functions.</td>
<td></td>
</tr>
</tbody>
</table>

### Detailed information about this topic

- My actions [on page 126](#)
- Auditing [on page 132](#)
- Governance administration [on page 133](#)

### My actions

**My Actions** is a submenu of Compliance. You can execute various actions to do with the compliance items you manage, depending on which entitlements you have been assigned. These actions can be called up over tiles.

### Detailed information about this topic

- Pending rule violations [on page 127](#)
- Rule violation history [on page 130](#)
- Pending policy violations [on page 130](#)
- Policy violations [on page 131](#)
Pending rule violations

Some rule violations can be approved as exceptions. You can see violations under your supervision in **Pending Rule Violations**. The following information is displayed in the corresponding menu.

**Table 40: Possible content of rule violations**

<table>
<thead>
<tr>
<th>Display</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>Employee who caused the rule violation.</td>
</tr>
<tr>
<td>Rule</td>
<td>Violated rule.</td>
</tr>
<tr>
<td>Approval state</td>
<td>The status of the approval. Following states are possible.</td>
</tr>
<tr>
<td></td>
<td>• Open</td>
</tr>
<tr>
<td></td>
<td>• Exception granted</td>
</tr>
<tr>
<td></td>
<td>• Exception denied</td>
</tr>
<tr>
<td>Approver</td>
<td>Employee who has denied or granted exception approval.</td>
</tr>
<tr>
<td>Approval date</td>
<td>Date of the approval decision.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>Shows the calculated risk index.</td>
</tr>
<tr>
<td>Risk index (reduced)</td>
<td>Shows the risk index reduced by the mitigating control.</td>
</tr>
<tr>
<td>Reason</td>
<td>Shows the manually entered reason added with the exception approval.</td>
</tr>
<tr>
<td>Standard reason</td>
<td>Displays a standard reason if one exist and this option was selected.</td>
</tr>
<tr>
<td>Valid until</td>
<td>The exception is only valid until this date.</td>
</tr>
</tbody>
</table>

If you are an auditor or an approver, you can obtain more information about exception approvals from **Auditing**. For more information, see **Rule violations** on page 132.

**To open the "Pending Rule Violations" menu**

- Open **Compliance | My Actions** and click **Pending Rule Violations**.

**Detailed information about this topic**

- **Approving exception approvals** on page 128
- **Resolving rule violations** on page 128
Approving exception approvals

As exception approver, you can grant or deny approval to exception approvals in Pending Rule Violations.

To grant or deny exception approvals

1. If rules have been violated, open Pending Rule Violations.
2. Use the filter function in Approval state and set Approval decision pending. Only the rule or policy violations of the selected type are displayed. For more information, see Filter on page 36.
3. Highlight the rule violation you want to approve in the list. This displays details of the violation in the detailed content view and you can carry out various actions. How you continue depends on the view you find yourself in.
4. Perform one of the following tasks:
   - Approve the request with ☑ and click Next.
   - Deny the violation with ☒ and click Next.
   Your selected is highlighted.
   This displays Approval exceptions.
5. Perform one of the following tasks:
   - Enter an reason for your approval decision.
   - Select a predefined reason.

   **NOTE:** You can optionally select a predefined text from Standard reasons for all cases still to be approved. Standard reasons are displayed in the approval history and in the case details. For more information about default reasons, see the One Identity Manager Compliance Rules Administration Guide or the One Identity Manager Company Policies Administration Guide.

   **NOTE:** If you are editing several rule or policy violations at the same time, you can enter a reason for each one individually.
6. Click Save.
   Your approval decision is saved and the rule or policy violation's status changes accordingly.

Resolving rule violations

As exception approver, you can edit violations of rule under your supervision. Rule violations are caused by permissions, so you have the option to remove permissions when you want to resolve one.
You can cancel the resolving process early because it is possible that you have removed other permissions while removing the violating permissions.

Permission assignments play an important role when editing rule violations. For example, permissions assigned through a dynamic role cannot be removed.

The following consequences may result from removing permissions:

### Table 41: Removing assigned permissions

<table>
<thead>
<tr>
<th>Assignment Method</th>
<th>Removing the Entitlement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct assignment</td>
<td>Direct assignment is deleted when the entitlement is removed.</td>
</tr>
<tr>
<td>Inherited assignment</td>
<td>The option to withdraw role membership from the employee is offered in the case of inherited permissions.</td>
</tr>
<tr>
<td>Dynamic assignment</td>
<td>Permissions cannot be removed if membership is through a dynamic role.</td>
</tr>
<tr>
<td>Assignment over IT Shop request</td>
<td>If permissions were assigned through a request, the request is canceled on removal.</td>
</tr>
<tr>
<td>Primary Assignment</td>
<td>The option to withdraw primary membership from the employee is offered in the case of permissions assigned through primary assignment.</td>
</tr>
</tbody>
</table>

**To resolve a rule violation**

1. Mark the rule violation and click **Resolve**.
   This opens the wizard "Resolve a rule violation", listing the permissions that led to the violation.

2. Mark the rule violation you want to remove from the employee in **Resolve a rule violation** and click **Next**.
   The objects is displayed with the permissions origin in **Verify**. The consequences of removing the permissions is displayed in **Action**.

3. Check whether you really want to delete the permissions and click **Next**.
   A message is displayed in **Loss of entitlement** and the permissions are listed that are affected by removal.

4. Perform one of the following tasks.
   a. To cancel the resolution of rule violations, choose **Cancel** or **Back**.
      All the employee's permissions remain intact.
   b. To continue with the resolution of the rule violation, choose **Continue**.
      All permissions that were displayed for resolving the rule violation are withdrawn from the employee.
Rule violation history

You can view exception approvals that you have dealt with in the Rule Violation History menu.

To view the history of your exception decisions

1. Open Rule Violation History for rule exceptions.
2. Use the filter function in the Approval state column and set the option Exception granted or Exception denied.
   Only historical rule or policy violations of the selected type are displayed. For more information, see Filter on page 36.
3. Select the rule or policy violation in the list.
   You can view more information in the detailed content view.

Detailed information about this topic

- Approving exception approvals on page 128
- Resolving rule violations on page 128

Pending policy violations

Some policy violations can be approved as exceptions. You can see violations under your supervision in Pending Policy Violations. The following information is displayed in the corresponding menu.

Table 42: Managing rule and policy violations

<table>
<thead>
<tr>
<th>Display</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violating object</td>
<td>Object, which caused the violation.</td>
</tr>
<tr>
<td>Policy</td>
<td>Violated policy.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the approval. Following states are possible.</td>
</tr>
<tr>
<td></td>
<td>• Open</td>
</tr>
<tr>
<td></td>
<td>• Exception granted</td>
</tr>
<tr>
<td></td>
<td>• Exception denied</td>
</tr>
<tr>
<td>Approver</td>
<td>Employee who has denied or granted exception approval.</td>
</tr>
<tr>
<td>Approval date</td>
<td>Date of the approval decision.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>Shows the calculated risk index.</td>
</tr>
</tbody>
</table>
### Display | Description
--- | ---
Risk index (reduced) | Shows the risk index reduced by the mitigating control.
Reason | Shows the manually entered reason added with the exception approval.
Standard reason | Displays a standard reason if one exist and this option was selected.
Valid until | The exception is only valid until this date.

If you are an auditor or an approver, you can obtain more information about exception approvals from **Auditing**. For more information, see **Rule violations** on page 132.

Some functions have already been described in the menu **Pending rule violations**. You can find all the functions available in this menu listed under "Detailed information about this topic".

**To open the "Pending Policy Violations" menu**
- Open **Compliance | My Actions** and click **Pending Policy Violations**.

**Detailed information about this topic**
- **Approving exception approvals** on page 128

### Policy violations

**To view the history of your exception decisions**

1. Open **Policy Violation History** for policy exceptions.
2. Use the filter function in the **Status** column and set the option **Exception granted** or **Exception denied**.
   - This limits the list of historical policy violations displayed to the selected option. For more information, see **Filter** on page 36.
3. Select a policy violation from the list.
   - You can view more information in the detailed content view.

**Detailed information about this topic**
- **Approving exception approvals** on page 128
Auditing

**Auditing** is a submenu of **Compliance**. You can execute various actions, such as viewing all requests or viewing all approved requests, depending on which entitlements you have been assigned. These actions can be called up over tiles.

**Detailed information about this topic**

- Rule violations on page 132
- Policy violations on page 132

**Rule violations**

<table>
<thead>
<tr>
<th>NOTE:</th>
<th>This function is only available if the module Company Policies Module or Compliance Rules Module is installed.</th>
</tr>
</thead>
</table>

All employees that have violated rules are displayed under **Rule violations**. **Auditing - Rule violations** shows you all rule violations within a selected time period. Rule violations that have been granted or denied exceptions or are pending are shown in **Rule violation**.

Some functions have already been described in the menu **Pending rule violations**. You can find all the functions available in this menu listed under "Detailed information about this topic".

**To open "Rule violations"**

- Open Compliance | Auditing and click **Rule violations**.

**Detailed information about this topic**

- Approving exception approvals on page 128
- Resolving rule violations on page 128

**Policy violations**

<table>
<thead>
<tr>
<th>NOTE:</th>
<th>This function is only available if the module Company Policies Module or Compliance Rules Module is installed.</th>
</tr>
</thead>
</table>

All employees that have violated policies are displayed under **Policy violations**. **Auditing - Policy violations** shows you all rule violations within a selected time period. Policy violations that have been granted or denied exceptions or are pending, are shown in **Pending policy violations**.
Some functions have already been described in the menu **Pending rule violations**. You can find all the functions available in this menu listed under "Detailed information about this topic".

**To open "Policy violations"**

- Open **Compliance | Auditing** and click **Policy violations**.

**Detailed information about this topic**

- Approving exception approvals on page 128

**Governance administration**

| NOTE: | This function is only available if Compliance Rules Module, Governance Base Module, Company Policies Module , or Attestation Module is installed. |

Companies have different requirements that they need for regulating internal and external employee access to company resources. On the one hand, rules are used for locating rule violations and on the other hand, to prevent them. They may also have to demonstrate that they adhere to legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance.

- Rule define to what permissions the employee has or otherwise. For example, a rule could prevent an employee from owning entitlement B if they already have entitlement A.

- Policies are very flexible, and can be defined around anything you are managing with Manager. For example, a policy could state that only managers in the HR department can have full control over a share on a file share that contains sensitive information.

- Each item to which an employee has access can be given a risk value. A risk index can be calculated for employees, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative: A request will not be processed if it is in violation, unless exception approvals are specifically allowed, and an approver allows it. Rules (if appropriate) and policies are run on a regular schedule, and violations appear on the appropriate employee’s Web Portal for handling. Policies may have associated mitigations, which are processes that an employee can do outside of the One Identity Manager solution to reduce the risks posed by the violation. Reports and dashboards give you further insights into your state of compliance. For more information, see **What statistics are available?** on page 263.

Which information you see in **Compliance** depends heavily on your role. If you do not see a menu item that you think you should, contact your system administrator. The following overview shows which view you can see for which user roles.
### Table 43: View "Compliance"

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-risk overview</td>
<td>Provides an overview of critical objects. The overview is divided into several parts.</td>
<td>Compliance and security officer</td>
</tr>
<tr>
<td>Compliance frameworks</td>
<td>Provided details about the compliance frameworks in your environment.</td>
<td>Compliance framework administrator</td>
</tr>
<tr>
<td>Rule violations</td>
<td>Provides reports on employees who violate policies.</td>
<td>Framework administrator, rule supervisor, and rule-exception approver</td>
</tr>
<tr>
<td>Policy violations</td>
<td>Provides reports on objects which violate policies.</td>
<td>Framework administrator, policy supervisor, and rule-exception approver</td>
</tr>
<tr>
<td>Rule analysis</td>
<td>Identifies employees who are in violation of rules related to SAP functions. You must configure SAP authorizations for testing. For more detailed information about SAP R/3 Compliance Add-on, see the One Identity Manager Identity Management Base Module Administration Guide.</td>
<td>Compliance framework administrator</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> the calculation of SAP functions must be activated by a manager.</td>
<td></td>
</tr>
<tr>
<td>Function analysis</td>
<td>Specifies employees whose access to high-risk SAP function violates the rules.</td>
<td>Rule supervisors</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> the calculation of SAP functions must be activated by an manager.</td>
<td></td>
</tr>
</tbody>
</table>

### Detailed information about this topic

- [Risk assessment](#) on page 135
- [High-risk overview](#) on page 264
- [Compliance frameworks](#) on page 136
- [Rule violations](#) on page 137
- [Policy violations](#) on page 138
- [Rule analysis](#) on page 138
- [Function analysis](#) on page 139
Risk assessment

Risk assessment is an important part of compliance. For example, high risk rule violations are more likely to require mitigations, or have fewer exception approvers. In One Identity Manager, risk data is gathered from a variety of sources, and then calculations are performed to produce risk indexes. Every item within One Identity Manager can be assigned a risk value. If you own resources, you maybe able to modify their risk values in the Master Data. For more information, see Master data on page 168.

In Risk Assessment, you can modify the risk index functions that are used to calculate these indexes. Risk indexes are calculated for employees, user accounts, system roles, IT Shop structures, organizations and business roles.

There are four calculation types that can be used. Choose the one that best fits the desired impact on risk for the risk index function you are modifying.

Table 44: Calculation types

<table>
<thead>
<tr>
<th>Calculation type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum (weighted)</td>
<td>The highest value from all relevant risk indexes is calculated, weighted and taken as basis for the next calculation.</td>
</tr>
<tr>
<td>Maximum (normalized)</td>
<td>The highest value from all relevant risk indexes is calculated, weighted with the normalized weighting factor and taken as basis for the next calculation.</td>
</tr>
<tr>
<td>Increment</td>
<td>The risk index of Table column (target) is incremented by a fixed value. This value is specified in Weighting/Change value.</td>
</tr>
<tr>
<td>Decrement</td>
<td>The risk index of Table column (target) is decremented by a fixed value. This value is specified in Weighting/Change value.</td>
</tr>
<tr>
<td>Average(weighted)</td>
<td>The average of all relevant risk indexes is calculated, weighted and taken as basis for the next calculation.</td>
</tr>
<tr>
<td>Average(normalized)</td>
<td>The average of all relevant risk indexes is calculated with the normalized weighting factor and taken as basis for the next calculation.</td>
</tr>
<tr>
<td>Reduction</td>
<td>Used when calculating the reduced risk index for compliance rules, SAP functions, company policies and attestation policies. You cannot add custom functions with this calculation type!</td>
</tr>
</tbody>
</table>

You can assign a weight to the calculation, which determines how much the result of a particular function affects the overall risk index. You can view high risk objects in High Risk Overview. For more information, see What statistics are available? on page 263.

To edit a risk index function

1. Open Compliance | Governance Administration and click Risk Assessment.
2. Mark the risk assessment function you want to view.
3. Click and select the required calculation type in the Attestation of assignment dialog.

4. Perform one of the following tasks:
   a. Use the slider to set a value between 0 and 1 on the Weighting/Change value scale.
      - OR -
   b. Check Disabled if you no longer want to use the risk index function.
      - OR -
   c. Uncheck Disabled if you want to use the risk index function again.

5. Click Save.

High-risk overview

This overview lists high-risk objects and divides them into different groups that can be expanded and collapsed. Each of the groups displays resources with the highest risk factor, which you manage. Risk indexes are calculated for employees, user accounts, system roles, structures, organizations, and business roles. Risk indexes are calculated for employees, user accounts, system roles, IT Shop structures, organizations and business roles, file systems, and SharePoint resources. Object have risk values, which provide the risk index when combined with risk index functions. You can view the following information in High-Risk Overview.

- Breakdown for of the highest-risk items for each type
- For more information on risk function calculators, see Modifying Risk Calculators.

Compliance frameworks

NOTE: This function is only available if at least one of the modules Governance Base Module, Attestation Module, Compliance Rules Module, or Company Policies Module is installed.

Compliance frameworks group together various policies, rules, and attestations to correspond with regulatory requirements. Compliance frameworks are set up by an administrator, but can be viewed in Web Portal.

This is required, for example, of you must comply to a certain framework. It is useful to know, which rules, policies and attestation policies are connected with the framework.

To view a compliance framework

- Open Compliance | Governance Administration and click Compliance Frameworks.
A Hyper View of the framework appears, with a shape for the associated rules, policies, and attestation policies.

**Rule violations**

Certain roles require you to find violations within their own system. This information can help to determine gaps in your security or compliance policies and help to develop attestation policies or violation mitigation. Mitigation comprises processes existing outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Governance administration on page 133.

You can generate reports that describe the rule violations exactly. These reports contain a risk assessment for you to use for prioritizing violations and on which to base subsequent planning. The reduced risk index takes into account many risk factors that arise from violations and represents the risk as a value between 0 (no risk) and 1 (high risk).

![NOTE:](image) You can only see Policy Violations or Rule Violations if you have the Compliance and Security Officer's or Auditor's application role.

Depending on which application is assigned to you, the following options are visible to you in your rule violation view:

- By framework
- By department
- By rule
- By application role
- All compliance rules

![NOTE:](image) If you only have one application role, you will not see any other options. The option corresponding to the application in this case is preset and must not be enabled by you.

**To view rule violations**

1. Open Compliance | Governance Administration and click Rule Violations.
2. Set one of the options shown to present the view more clearly.
3. Mark a rule.
4. Get further information.
5. Perform one of the following tasks:
   a. Click of the links in the detailed content view to display more details.
   b. Click "Show details" to display details about the selected rule.
   c. Depending on your role assignments, you can generate a report using Report.
Policy violations

Certain roles require you to find policy violations within their own system. This information can help to determine gaps in your security or compliance policies and help to develop attestation policies or violation mitigation. Mitigation comprises processes existing outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Governance administration on page 133.

You can generate reports, which exactly describe the rule or policy violations. These reports contain a risk assessment for you to use for prioritizing violations and on which to base subsequent planning. The reduced risk index takes into account many risk factors that arise from violations and represents the risk as a value between 0 (no risk) and 1 (high risk).

NOTE: You can only see the Policy violations or Rule violations if you have the compliance and security officer’s or auditor’s application role.

Depending on which application roles have been assigned to you, the following options are visible to you in your rule violation view:

- Framework administrator
- Policy supervisors
- Exception approvers
- All Policies

NOTE: If you only have one application role, you will not see any other options. The option corresponding to the application in this case is preset and must not be enabled by you.

To view rule violations

1. Open Compliance | Governance Administration and click Policy Violations.
2. Set one of the options shown to present the view more clearly.
3. Mark a rule.
4. Get further information.
5. Perform one of the following tasks:
   a. Click of the links in the detailed content view to display more details.
   b. Click "Show details" to display details about the selected rule.
   c. Depending on your role assignments, you can generate a report using Report.

Rule analysis

Users who have access to certain critical SAP functions, may violate compliance rules and can pose a significant security threat. You should analyze these users to determine if action
should be taken. Two menus help you with these tasks in the Web Portal. Rule analysis shows compliance rules that contain SAP functions and identify each employee that violates the rules. You can analyze the rule violation to determine the cause.

**To obtain information about SAP user accounts involved in violating rules.**

1. Select **Compliance | Governance Administration** and click **Rule analysis**.
   A list of compliance rules including SAP functions appears.
2. Click **Select** in the required entry to display the user accounts and employees related to the violated compliance rule.
   You can determine which rules have violations by using the Critical Function Analysis.
   For any employee who has violated the rule, you can analyze the violation by role or ability.
3. Perform one of the following tasks:
   a. Click **By role** in the required entry to expand details about roles and profiles for the rule violation.
   b. Click **By ability** in the required entry to expand details about the SAP functions and transactions.
   c. Click **Back** to return to the list of employees.

**Function analysis**

Function analysis shows you employees with critical SAP functions that violate compliance rules. For each employee, you can determine what SAP function is involved in the violation and the rules that caused the violation. You can use the significance rating to prioritize your actions. If a rule with a significance rating is violated by an SAP function with a significance rating it must be handled promptly.

**To identify employees who violate compliance rules with critical SAP functions.**

1. Select **Compliance | Governance Administration** and click **Critical function analysis**.
   A list of employees who have certain critical SAP functions is displayed.
2. Click **Select** in the requested entry to display the SAP functions and rule violations for the selected employee.
Ownerships

In **Responsibilities**, you can run various actions and obtain information. The following tables provide you with an overview of the menu items and actions that can be executed here.

**Table 45: Menu items for "Responsibilities"**

<table>
<thead>
<tr>
<th>Menu item</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My responsibilities</td>
<td></td>
<td><strong>Employees</strong> View your employees and their details. Add new people.</td>
</tr>
<tr>
<td>Menu item</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Resources</td>
<td>View your resources and their details. Add new resources.</td>
<td></td>
</tr>
<tr>
<td>Assignment resources</td>
<td>View and edit your assignments resources and their details. Add entitlements and view historical data.</td>
<td></td>
</tr>
<tr>
<td>Multi-requestable/un-subscribable resources</td>
<td>View and edit Multi-requestable/unsubscribable resources and their details. Request memberships for employees and add permissions. View historical data.</td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td>View and edit your devices. Add new devices.</td>
<td></td>
</tr>
<tr>
<td>Task delegation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delegation</td>
<td>View those responsibilities you can delegate.</td>
<td></td>
</tr>
<tr>
<td>Delegation history</td>
<td>View your delegations to other staff and delegate responsibilities to them.</td>
<td></td>
</tr>
<tr>
<td>Ownerships</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claim ownership</td>
<td>Claim responsibility for a group that does not has no one in charge.</td>
<td></td>
</tr>
<tr>
<td>Assigning owners</td>
<td>Assigns an owner to a business object.</td>
<td></td>
</tr>
<tr>
<td>Auditing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Departments</td>
<td>View one or all departments of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>View one or all applications of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>Business roles</td>
<td>View one or all business roles of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>Cost centers</td>
<td>View one or all cost centers of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>Multi-request resources</td>
<td>View one or all multi-request resources of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>Employees</td>
<td>View all employee details.</td>
<td></td>
</tr>
<tr>
<td>One Identity Manager application roles</td>
<td>View one or all application roles of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>Resources</td>
<td>View one or all resources of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>Menu item</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Locations</td>
<td>View one or all locations of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>System roles</td>
<td>View one or all system roles of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>Assignment resources</td>
<td>View one or all assignment resources of the employee who is responsible for them.</td>
<td></td>
</tr>
<tr>
<td>Active Directory</td>
<td>View one or all entitlements of the employee who is responsible for a Active Directory group.</td>
<td></td>
</tr>
<tr>
<td>Azure Active Directory</td>
<td>View one or all entitlements of the employee who is responsible for a Azure Active Directory group.</td>
<td></td>
</tr>
<tr>
<td>G Suite</td>
<td>View one or all entitlements of the employee who is responsible for a G Suite group.</td>
<td></td>
</tr>
<tr>
<td>IBM Notes</td>
<td>View one or all entitlements of the employee who is responsible for a IBM Notes group.</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>View one or all entitlements of the employee who is responsible for a LDAP group.</td>
<td></td>
</tr>
<tr>
<td>Privileged Account Management</td>
<td>View one or all entitlements of the employee who is responsible for a Privileged Account Management group.</td>
<td></td>
</tr>
<tr>
<td>SAP R/3</td>
<td>View one or all entitlements of the employee who is responsible for a SAP R/3 group.</td>
<td></td>
</tr>
<tr>
<td>Universal Cloud Interface</td>
<td>View one or all entitlements of the employee who is responsible for a Universal Cloud Interface group.</td>
<td></td>
</tr>
<tr>
<td>UNIX</td>
<td>View one or all entitlements of the employee who is responsible for a Unix group.</td>
<td></td>
</tr>
</tbody>
</table>

**Governance administration**

| Business roles | View and edit business roles and their details. Restore deleted roles. Split up, compare or merge roles. |
| System entitlements | View and edit system entitlements and their details. Add members, assign devices, and view historical data. |
Detailed information about this topic

- My responsibilities on page 143
- Task delegation on page 218
- Ownerships on page 222
- Auditing on page 224
- Governance administration on page 238

My responsibilities

The My Responsibilities view is a submenu of the Responsibilities menu. Here you can view the tasks and entitlements under your supervision within your company. You can manage the following responsibilities: These actions can be called up over tiles.

- Employees
- Devices
- Hierarchical roles
  - Organizations
    - Departments
    - Cost centers
    - Locations
  - Business roles
- Company resources
  - System roles
  - System entitlements
  - System entitlements
  - Application roles
  - Resources
  - Assignment resources
  - Multi-request resources
  - Multi-requestable/unsubscribable Resources
  - Applications

Related topics

- Employees on page 144
- System entitlements on page 158
Employees

You can add new people over the People menu. This function is mainly designed for adding external employees. For example, subcontractors who are not entered in the human resources department. Data from new employees is either transferred completely to the database or existing data is updated and/or augmented. This depends on the system configuration and the import setting from closed systems.

To open the "People" menu

- Open the menu Responsibilities | My Responsibilities and click People.

Detailed information about this topic

- Adding employees on page 145
- Viewing rule violations on page 146
- Editing employee data on page 147
- Assigning new managers on page 148
- Creating a passcode on page 148
- Creating reports about employee data on page 149
- Displaying information on page 145
- Viewing risk indexes on page 149
- Adding new delegations on page 149
- Deleting or canceling delegations on page 151
- Displaying and deleting memberships on page 151
- Displaying assignment of an entitlement on page 151
Displaying information

On the **Responsibilities | My Responsibilities** page, in an overview, you can view a summary of all the relevant information about an object for which you are responsible. This information includes, for example, people, their request, rule violations, user accounts, subidentities, assigned permissions and memberships. They are displayed in shape elements.

**To view an object's overview**

1. In the menu bar, click **Responsibilities | My Responsibilities**.
2. On the **My Responsibilities** page, click the **People** tile.
3. On the **People** page, click on the employee you want to view.
4. On the overview page of this employee, click the **Overview** tile.

Adding employees

You can add new employees in the **People** menu.

**To add a new employee**

1. In the menu bar, click **Responsibilities | My Responsibilities**.
2. Open **People** and click **Add a new employee**.
3. Enter the required data in the text and selection fields and click **Save**.
   
   Fields marked with * are compulsory. When saving, the system checks whether the combination of first and last name already exists.

   There are different use cases that require different input sequences. The following tables layout the use cases and the respective input sequences.

**Table 46: Use cases and input sequences when adding a new employee**

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Input Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>If this combination of first and last</td>
<td>1. Confirm the prompt with <strong>OK</strong>.</td>
</tr>
<tr>
<td>Use Case</td>
<td>Input Sequence</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>name does not exist, you will be prompted to save the changes.</td>
<td>This adds the new employee.</td>
</tr>
<tr>
<td></td>
<td>2. Save the changes.</td>
</tr>
<tr>
<td>If this combination of first and last name already exists, they are</td>
<td>Other employees with similar properties.</td>
</tr>
<tr>
<td>listed in the view</td>
<td>In this case, you have two possible options.</td>
</tr>
<tr>
<td>If the employee you want to add is already in the list, you can select</td>
<td>1. Mark the employees in the list whose data you want to use and click</td>
</tr>
<tr>
<td>this data record and edit it. Proceed as follows.</td>
<td>Update employee data.</td>
</tr>
<tr>
<td></td>
<td>This displays a message and you are prompted to save the changes.</td>
</tr>
<tr>
<td></td>
<td>2. Confirm the prompt with OK.</td>
</tr>
<tr>
<td></td>
<td>The new employee data is added with the existing data. You can edit or</td>
</tr>
<tr>
<td></td>
<td>change the data.</td>
</tr>
<tr>
<td></td>
<td>3. Save the changes.</td>
</tr>
<tr>
<td>Another option is to add new data despite the duplicate data record.</td>
<td>1. Click Add a new employee.</td>
</tr>
<tr>
<td></td>
<td>A message is displayed and you are asked whether you want to add a new</td>
</tr>
<tr>
<td></td>
<td>employee.</td>
</tr>
<tr>
<td></td>
<td>2. Confirm the prompt with OK.</td>
</tr>
<tr>
<td></td>
<td>This adds the new employee.</td>
</tr>
<tr>
<td></td>
<td>3. Save the changes.</td>
</tr>
</tbody>
</table>

**Viewing rule violations**

You can view rule violations for your staff in the People menu.

**To view your staff’s rule violations**

1. In the menu bar, click **Responsibilities | My Responsibilities**.

2. Open the **People** menu and click **Rule violations**.

   In the Rule violations from direct subordinates view, you can see the rule violations caused by your staff. The following information is listed in the view.
### Table 47: Columns in "Rule violations by direct reports" view

<table>
<thead>
<tr>
<th>Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>Name of the supervised employee</td>
</tr>
<tr>
<td>Rule violation</td>
<td>Unique rule violation ID.</td>
</tr>
<tr>
<td>Checked</td>
<td>Shows whether the rule violation was tested.</td>
</tr>
<tr>
<td>Exception is approved</td>
<td>Shows whether an exception was approved for the rule violation.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>Shows the calculated risk index.</td>
</tr>
<tr>
<td>Risk index (reduced)</td>
<td>Shows the reduced risk index.</td>
</tr>
<tr>
<td>Approval date</td>
<td>Shows the approval date, if the rule violation was already checked.</td>
</tr>
<tr>
<td>Reason</td>
<td>Shows a reason for the approval decision about the rule violation.</td>
</tr>
</tbody>
</table>

Use the View Settings | Additional columns to show more columns in the view. The following columns are available.

### Table 48: Additional columns for "Compliance rule violations by direct reports"

<table>
<thead>
<tr>
<th>Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approver</td>
<td>The name of the approver checking the rule.</td>
</tr>
<tr>
<td>Valid until</td>
<td>Date specifying for how long the rule violation applies.</td>
</tr>
<tr>
<td>Standard reason</td>
<td>Default reason available for all rule violations. Multiple use is possible.</td>
</tr>
</tbody>
</table>

### Editing employee data

You can edit your staff’s data in the People menu.

**To view and edit employee data**

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Open People.
3. Use a filter and then mark the item you want in the result list.
4. Make the changes under Master data and click Save.
Assigning new managers

In the People menu, you can assign new managers to your staff in their master data.

To assign an employee to a new manager

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Open the People menu and select an employee.
3. Select Master data and click Assign to new manager.
4. Select a new manager via Change.
5. Enable the checkbox in Assign to new manager and set a time and date from which the new manager takes effect.

   NOTE: If the employee with the new manager already has approved requests or entitlements, they are deleted automatically on this date. If you want the employee to retain these requests or entitlements when transferring to the new manager, disable the Delete on the effective date or Cancel on the effective date.

6. Click Submit and choose OK to confirm.

   Your changes are saved and the message Your manager change request has been submitted. is displayed in the employee’s Master data.

   NOTE: Your request to change managers is presented for approval in the Pending Requests menu of the approver responsible.

Creating a passcode

If one of your staff has forgotten their password for logging into the Web Portal and the password cannot be reset with the question and answer function, you can create a passcode for them.

The passcode can only be used once and is only valid for a limited time period.
To create a passcode for an employee

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Open the People menu and select an employee.
3. Click Passcode.
   The generated passcode and its validity are displayed in a dialog.
4. Note or mark the code and send it and the validity period to the employee.

Creating reports about employee data

In People, you can create a report with the data from one of your staff.

To create a report

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Open Employee.
3. Use a filter and then mark the item you want in the result list.
4. Open Master data and click Generate report.
5. Perform one of the following tasks:
   - Enable Create a report with history.
   - Enable Include data for sub identities in the report.
6. Click Generate report.

Viewing risk indexes

You can view the risk index for any member of your staff in the My Responsibilities menu.

To view the risk index

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Open the People menu and select an employee.
3. Select Risk to view the risk index assessment view and click View risk functions.

Adding new delegations

In the People menu, you can an employee's delegate roles or responsibilities to another employee. You can delete or cancel delegations that have already been made.
To add a delegation

1. In the menu bar, click **Responsibilities | My Responsibilities.**
2. Open the **People** menu.

   **NOTE:** There is a filter to help you search for a particular employee.
3. Select the employee for delegation.
4. Click the **Delegations** tile.
5. On the **Delegations** page, click **New delegation.**
6. In the **Delegation of role memberships and responsibilities** dialog, use **Assign** to select an employee for delegation.
7. Click **Next.**
8. Select one or more roles/responsibilities and click **Next.**
9. Configure the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid from</td>
<td>Start date and time of the delegation.</td>
</tr>
<tr>
<td>Valid until</td>
<td>Expiry date and time of the delegation.</td>
</tr>
<tr>
<td>Notify me if the recipient of the delegation makes a decision.</td>
<td>If the option is set, you receive a message in this case.</td>
</tr>
<tr>
<td>The recipient can delegate this role</td>
<td>If the option is set, the recipient of the delegation can delegate the role to someone else.</td>
</tr>
<tr>
<td>Reason</td>
<td>Field for entering a reason for delegating.</td>
</tr>
<tr>
<td>Priority</td>
<td>Menu for selecting a priority. The following priorities are available:</td>
</tr>
<tr>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td></td>
<td>• High</td>
</tr>
<tr>
<td></td>
<td>• Medium</td>
</tr>
<tr>
<td></td>
<td>• Low</td>
</tr>
</tbody>
</table>

10. Click **Save.**
Deleting or canceling delegations

You can delete or cancel delegations in People.

To delete or cancel a delegation

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Open Employee.

   NOTE: There is a filter to help you search for a particular employee.
3. Select the employee for delegation.
4. Click the Delegations tile.
5. On the Delegations page, perform one of the following tasks:
   - In the Delete column, click for the relevant delegations and then Actions | Delete delegation.
   - Click Actions | Delete all delegations.
   - Select the delegation and click Withdraw request in the main detail view.

Displaying and deleting memberships

You can view your staff’s memberships in the People menu and delete existing memberships. These memberships are, for example, assigned entitlements or roles.

To view an employee’s memberships and delete them.

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Open the People menu.
3. Use a filter and then mark the item you want in the result list.
4. Click the Entitlement tile.
5. On the Entitlements page, mark the memberships you want to view and look at the details in the detailed content view.
6. Check the box in front of the membership you want to delete.
7. Click Delete memberships.

Displaying assignment of an entitlement

In the People menu you can view entitlement assignments in the Entitlements view.
To view an entitlement assignment

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click People.
3. Open Employee.
4. On the People page, click on the employee whose entitlements you want to view.
5. Click the Entitlement tile.
   
   **NOTE:** The option Edit memberships must be set.

6. On the Entitlements page, mark the desired entitlement.
7. In the detailed content view, click next to the Analysis for item.
   This finds all the roles the employee belongs to. You can also see how the roles have been assigned. For example, roles might be assigned directly.

Requests

This view shows all the products that the employee has requested, or that have been requested for them, or by another employee, for example, a manager.

To search for a specific approval decision by approval

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Open Employee.
3. Use a filter and then mark the item you want in the result list.
4. Click the Request tile.
5. Perform one of the following tasks:
   a. Use a filter and then mark the item you want in the result list.
   b. Mark the entry you want in the list.
   This displays details of the selected item in the detailed content view.

History

You can view history data for objects you manage in My Responsibilities. You can use History to see changes to a base object over time. It shows states and comparisons of base object attributes.

The history is divided into three views.
Table 50: History views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>Displays all events affecting the base object, on a timeline. This is the default History view.</td>
</tr>
<tr>
<td>Status overview</td>
<td>Displays a list of modified properties with their validity period and dates when they were changed.</td>
</tr>
<tr>
<td>Status comparison</td>
<td>Displays the differences between in the current and selected time point.</td>
</tr>
</tbody>
</table>

**To open the history**

1. In the menu bar, click **Responsibilities | My Responsibilities**.
2. Open the **People** menu and select an employee.
3. Select **History**.
4. Open **Locations** and select a location.

**Timeline**

In the history's **Timeline** view, you can run different actions and configure settings to view events from the past to the present. The following table explain the options.

<table>
<thead>
<tr>
<th>Action</th>
<th>Input Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move backward or forward</td>
<td>1. Click the timeline and hold down the left mouse key.</td>
</tr>
<tr>
<td></td>
<td>2. Perform one of the following tasks:</td>
</tr>
<tr>
<td></td>
<td>a. Drag the marking to the left to go forward in time on the timeline.</td>
</tr>
<tr>
<td></td>
<td>b. Drag the marking to the right to go back in time on the timeline.</td>
</tr>
<tr>
<td>Change the display within the timeline</td>
<td>• Turn the mouse wheel to zoom in or zoom out.</td>
</tr>
<tr>
<td></td>
<td>The timeline view can vary from months to hours.</td>
</tr>
<tr>
<td>Switch to table view</td>
<td>• Click <strong>Switch to table view</strong> below the timeline.</td>
</tr>
<tr>
<td></td>
<td>This switches views and the same data is shown in a table. The table displays the change type, property, new and old value of the change and the date of change, amongst others. To return to the timeline view, click <strong>Switch to timeline view</strong>.</td>
</tr>
<tr>
<td>View event details</td>
<td>• Click one of the colored elements on the timeline to view a particular event in more detail.</td>
</tr>
</tbody>
</table>
### Action: Apply filter

#### Input Sequence

1. Click **Filter by...** and select an entry from the following.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Searches for events or actions associated with the given name. Employees with entitlements and owner- ships create changes, such as adding or removing properties. You can view these actions on the timeline.</td>
</tr>
<tr>
<td>Change type</td>
<td>Lists all changes types, which can be selected for displaying in the timeline. Multi-select is possible.</td>
</tr>
<tr>
<td>Date</td>
<td>List all actions and events for the selected date.</td>
</tr>
<tr>
<td>Property</td>
<td>Lists all properties, which can be selected for displaying in the timeline. Properties are, for example, employee, manager or dynamic role. For more detailed information about assigning through dynamic roles, see the One Identity Manager Identity Management Base Module Administration Guide. Multi-select is possible.</td>
</tr>
<tr>
<td>Display</td>
<td>Searches for all text data matching the given search term. The following settings are available.</td>
</tr>
<tr>
<td></td>
<td>- All words</td>
</tr>
<tr>
<td></td>
<td>- Starts with...</td>
</tr>
<tr>
<td></td>
<td>- Ends with...</td>
</tr>
<tr>
<td></td>
<td>- One or more words</td>
</tr>
</tbody>
</table>

2. Apply the selected filter with **Filter on**.

### Status comparison

In the history's **Status comparison**, you can compare the current status of objects with other points in the past.
To compare object statuses

- Perform one of the following tasks:
  - Click **Compare** in the event dialog, if you have clicked on the event on the timeline.
    This compares the current object status with the point of the selected event and displays the result in **Status comparison**.
  - Select **Status comparison** and click next to the field to select the date.

The statuses and comparisons displayed in the history overview are dependent on the type of base object selected. The following attributes can be displayed.

**Table 51: Overview of base objects and their attributes**

<table>
<thead>
<tr>
<th>Base object type</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>Change of base object property</td>
</tr>
<tr>
<td></td>
<td>Responsibility for an employee</td>
</tr>
<tr>
<td></td>
<td>Responsibility for a department</td>
</tr>
<tr>
<td></td>
<td>Responsibility for a cost center</td>
</tr>
<tr>
<td></td>
<td>Responsibility for a location</td>
</tr>
<tr>
<td></td>
<td>Membership in an application role</td>
</tr>
<tr>
<td></td>
<td>Membership in a department</td>
</tr>
<tr>
<td></td>
<td>Membership in a cost center</td>
</tr>
<tr>
<td></td>
<td>Membership in a location</td>
</tr>
<tr>
<td></td>
<td>Assignment to a resource</td>
</tr>
<tr>
<td></td>
<td>Application assignment</td>
</tr>
<tr>
<td></td>
<td>Identifying a compliance rule violation</td>
</tr>
<tr>
<td></td>
<td>Assignment to a business role</td>
</tr>
<tr>
<td></td>
<td>Responsibility for a business role</td>
</tr>
<tr>
<td></td>
<td>Responsibility for a system role</td>
</tr>
<tr>
<td></td>
<td>Assignment to a system role</td>
</tr>
<tr>
<td></td>
<td>Assignment to a target system account</td>
</tr>
<tr>
<td>Department</td>
<td>Change of base object property</td>
</tr>
<tr>
<td>Cost center</td>
<td>Employee membership</td>
</tr>
<tr>
<td>Location</td>
<td>Assignment to a resource</td>
</tr>
<tr>
<td>Business role</td>
<td>Assignment to a system role</td>
</tr>
</tbody>
</table>
Comparing an employee's status

In the My Responsibilities menu, you can compare the current status of an employee with a status from the past in the History view. This compares attributes, which have changed within a specified time period. You specify the time period yourself in the date control provided.

This comparison is also available for company structures.

To run a comparison of an employee's status

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Open the People menu and select an employee.
3. Select the Status comparison view under History.
4. Click  and  to select a date and time with which you want to compare the employee's current status.

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

NOTE: You can apply a filter to all columns in the view. For more information, see Filter on page 36.

Attestations

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

In the Attestation view under Employee, you can see your employee's attestation cases. You will see both attestation cases approved or denied by you and pending attestation.

In Attestations, you can switch between different views.

- Group memberships
- Objects attestation
- All attestation cases

For each case you can see the current status and the creation date in the detailed content view. You can run the following action or get information.

- See whether the case was approved or denied.
- Obtain detailed information about the selected attestation case from the Information, Workflow, Attestation policy and History tabs.
- As attestor, you can view attestors for pending attestation cases.
- Send a reminder.
- Approve attestation cases for object attestations as approver.
Approving attestations

In the **Employee** menu under **Attestation**, you can make approval decisions for employee's pending attestations.

**NOTE:** You can also make approval decisions in **Pending Attestations**.

**To approve pending attestations**

1. In the menu bar, click **Responsibilities | My Responsibilities**.
2. Open **Employee**.
3. Use a filter and then mark the item you want in the result list.
4. Select **Attestations** and open either **Object attestation** or **All attestation cases**.
5. Select **Approve**.
   This opens **Pending attestations**.
6. In the pending attestations view, select the required case.
7. Perform one of the following tasks:
   - Grant approval by clicking ✅.
   - Deny approval by clicking ❌.
8. If required, repeat step 3 and click **Next**.
9. Perform one of the following tasks:
   - Enter a reason for your decision in the field.
   - Select an available reason in the **Standard reason** field.

**NOTE:** You have the option of selecting a predefined text for all cases still to be approved using the **Standard reason** menu. Standard reasons are displayed in the approval history and in the case details. For more detailed information about default reasons, see the One Identity Manager Attestation Administration Guide.

10. Click **Save**.

**NOTE:** Some attestation cases that still need to be approved, require multi-factor authentication. After your approval decision has been saved, you will prompted to enter a security code. For more information, see **Requesting products that require multi-factor authentication** on page 81.
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.

The following system entitlements, for example, are displayed on the System entitlement page:

- Active Directory groups
- SAP groups
- SharePoint groups
- Privileged Account Management groups

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

- View a variety of information about the system entitlement (in a Hyper View), its members, attestation cases and usage of the different role classes.
- Add a new owner role and assign a product owner to an Active Directory group if you are target system administrator. You can also edit the requestability of an Active Directory group.
- Change the properties of the entitlement.
- Add members to system entitlements.
- Obtain an overview of all groups that are members of a system entitlement.
- Analyze that state and compare attributes of the base object. You can perform this task in the historical data view.

To show system entitlements

1. In the menu bar, click Responsibilities | My Responsibilities.
2. Click the System entitlements tile.

Detailed information about this topic

- Displaying information on page 145
- Adding memberships on page 159
- Deleting memberships on page 160
- Editing master data on page 160
- Attestations on page 161
- Owner on page 162
- New owner role on page 162
- Moving responsibilities on page 163
- Usage on page 163
Adding memberships

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

You can add members to roles, organizations, and entitlements for which you are responsible and have the required access. This is an alternative to making a request for membership on behalf of an employee.

You can delete memberships as well as adding them.

NOTE: Employees cannot be assigned to assignment resources.

To request new membership
1. Perform one of the following tasks:
   - Under **System entitlement**, open **Memberships** for the required system entitlement.
   - Under **Business roles**, open **Memberships** for the required business role.
   - Under **System roles**, open **Memberships** for the required system role.
   - Under **Departments**, open **Memberships** for the required department.
   - Under **Cost centers**, open **Memberships** for the required cost center.
   - Under **Locations**, open **Memberships** for the required location.
   - Under **Resources**, open **Memberships** for the required resources.
   - Under **Assignment resources**, open **Memberships** for the required resource.
   - Under **Multi-request resources**, open **Memberships** for the required resource.
   - Under **Multi requestable/unsubscribeable resources**, open **Memberships** for the required resource.
2. Click **Request memberships**.
3. Select the required employee (multi select is permitted) and click **Move to shopping cart**.
Your shopping cart appears. For more information, see Edit shopping cart on page 78.

Deleting memberships

Deleting memberships is similar to a requests workflow. You can delete members from roles, organizations, and entitlements for which you are responsible and have the required access. The assignment is removed by the deletion process.

NOTE: Employees cannot be assigned to or deleted from assignment resources.

To delete a membership

1. Perform one of the following tasks:
   a. Under System entitlement, open Memberships for the required system entitlement.
   b. Under Business roles, open Memberships for the required business role.
   c. Under System roles, open Memberships for the required system role.
   d. Under Departments, open Memberships for the required department.
   e. Under Cost centers, open Memberships for the required cost center.
   f. Under Locations, open Memberships for the required location.
   g. Under Resources, open Memberships for the required resources.
   h. Under Assignment resources, open Memberships for the required resource.
   i. Under Multi-request resources, open Memberships for the required resource.
   j. Under Multi requestable/unsubscribable resources, open Memberships for the required resource.
   k. Under Applications, open Memberships for the required application.

1. Click Delete memberships.
   This deletes the membership.

Editing master data

You edit master data in System Entitlements if you want to edit requestability settings.

NOTE: This function is only available if the module Active Roles Module is installed.
To change the master data of a group managed by an Active Roles

1. Open System entitlements and select the required system entitlement managed by a Active Roles.
2. Select Master data.
3. Perform one of the following tasks:
   - Enable Only use in IT Shop.
   - Enable Approval by the owner of the group.
   - Enable Approval by a additional owner of the group.
   - Choose Change to select a different service item.

Attestations

You can view pending attestation on your system entitlements.

In the Attestation view, you can switch between the following views and see membership attestations in system entitlements or system roles. Which views you see, depends on the selected company structure.

In Attestations, you can switch between different views.

- Memberships
- Group memberships
- Objects attestation
- All attestation cases

For each case you can see the current status and the creation date in the detailed content view. You can run the following action or get information.

- See whether the case was approved or denied.
- Obtain detailed information about the selected attestation case from the Information, Workflow, Attestation policy and History tabs.
- As attestor, you can view attestors for pending attestation cases.
- Send a reminder.

To view attestations of the desired area of responsibility

1. Perform one of the following tasks:
   - Open System entitlements and select a system entitlement.
   - Open the System Roles menu and select a system role.
2. Select Attestations.
Detailed information about this topic

- Viewing details on page 103
- Attesting pending attestations on page 103
- Sending reminders on page 104

Owner

NOTE: This function is only available if the module Active Directory Module is installed.

In the System entitlements menu, you can assign new product owners to Active Directory groups.
But you can also create a new owner role or move responsibilities.

To change the product owner of an Active Directory.

1. Open System entitlements and select the required Active Directory group.
2. Select the Owner view and click Change.
3. Select another product owner from the list.

New owner role

NOTE: This function is only available if the module Active Directory Module is installed.

In the System entitlements menu, you can assign new product owners to Active Directory groups.

To assign a new product owner to an Active Directory group

1. Open System entitlements and select the required Active Directory group.
2. Select Owner and click New.
   
   NOTE: Before you can assign a new product owner, you must add a new owner role for this employee.

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

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

4. Use the Assign link to select a new product owner and select the new owner role via the Product owner link.

   NOTE: If Without owner in AD was selected in Product owner, you cannot select a product owner.
Moving responsibilities

NOTE: This function is only available if the module Active Directory Module is installed.

In the System entitlements menu, you can move all owners of a role to a new owner role.

To change the product owner of an Active Directory.

1. Open System entitlements and select the required Active Directory group.
2. Select Owner and click Move ownership.
   This opens Move ownership to new owner role with the note that a new owner role will be added.
3. Set Move all owners in the dialog if you want to move all owner to the new role.

Attestors

In System entitlements, you can change attestors at Active Directory groups. But you can also create a new attester or move responsibilities.

NOTE: Before you can assign a new attester, you must add a new application role.

To assign an attester to an Active Directory group

1. Open System entitlements and select the required Active Directory group.
2. Select Attestors.
3. Perform one of the following tasks:
   a. Click Change.
   b. Select another attester from the list.
      - OR -
   a. Click New.
   b. Enter a name for the new application role and a reason for creating it.
   c. Select an attester using the Assign link and the new application role using the Attestor link.

Usage

Roles are used to help manage assignments to employees. For example, instead of assigning many resources separately to an employee, you can add them to a role that inherits the proper assignments from a role class. A role class is the highest level, and
roles can be nested in it. In **Usage**, you see all role members that can be a member of the selected entry. If you select a role class, you can view all the members with a role.

Information is displayed as a hierarchical chart, so you can drill in and see the role inheritance.

**MOBILE:** This function is not available in the mobile interface.

**To view employee assignments of a role class**

1. Perform one of the following tasks:
   a. Open **System entitlements** and select a system entitlement.
   b. Open **Business Roles** and select a business role.
   c. Open the **System Roles** menu and select a system role.
   d. Open **Department** and select a department.
   e. Open **Cost Center** and select a cost center.
   f. Open **Locations** and select a location.
   g. Open **Resources** and select a resource.
   h. Open **Assignment resources** and select a resource.
   i. Open **Multi-request resources** and select a resource.
   j. Open **Multi requestable/unsubscribable resources** and select a resource.
   k. Open **Applications** and select an application.

2. Select **Usage**.
3. Select a role class.
   This displays employee assignments for the selected role class.
4. Open the legend for the selected role class with **More information**.

**Child groups**

Some groups own group memberships. The **Child groups** view is only available for these groups. Not only do you have an overview of existing group memberships, you can also add them. For this, you assign a child group to the selected group. The following groups can, for example, own group memberships or allow assignment of child groups.

- Active Directory groups
- SAP groups

In the following step-by-step, adding a group membership is described on the basis of an Active Directory group.
**To assign a child group to a group**

1. Open **System entitlements** and select an Active Directory group.
2. Select **Child groups** and click **New child group**.
3. Select a child group using **Assign** and save it.
   The selected child group is displayed in **Child groups**.

**Business roles**

1. **NOTE:** This function is only available if the module Business Roles Module is installed.

Business roles are defined based on the resources needed to perform a particular function. The roles that appear on this list are roles that you are responsible for administering.

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

- View information about the business role, members and entitlements, risk assessment and rule violations, attestation cases and usage of various role classes.
- Change the properties of the role.
- Add members to the role.
- Add entitlements to the role.
- View statistics.

1. **NOTE:** As administrator, you can view and edit all business roles in the **Business Roles** view by clicking on the link provided.

Some functions have already been described in other menus. You can find all the functions available in this menu listed under "Detailed information about this topic".

**To open the "Business Roles" menu**

- Open the menu **Responsibilities | My Responsibilities** and click **Business Roles**.

**Detailed information about this topic**

- **Displaying information** on page 145
- **New business roles** on page 166
- **Restoring deleted roles** on page 240
- **Master data** on page 168
- **Adding memberships** on page 159
- **Deleting memberships** on page 160
- **Adding entitlements** on page 169
New business roles

In Business Roles, you can add new business roles. To do this, you enter the master data.

To add a new business role

1. Open Business roles and click New business role.
2. Set the following in Create a new business role and click Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business role</td>
<td>Field for a business role.</td>
</tr>
<tr>
<td>Short name</td>
<td>Field for a shorten name.</td>
</tr>
<tr>
<td>Internal name</td>
<td>Input name for the internal name.</td>
</tr>
<tr>
<td>Role class</td>
<td>Menu for selecting the role class</td>
</tr>
<tr>
<td>Parent business role</td>
<td>Link for selecting the parent business role</td>
</tr>
<tr>
<td>Role type</td>
<td>Menu for selecting the role type.</td>
</tr>
</tbody>
</table>

NOTE: Any fields that are not marked with an asterisk (*) are optional. Optional fields can be filled in when you create the application or at a later stage.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role approver</td>
<td>Link for selecting an application role as approver</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Link for selecting an application role as approver (IT)</td>
</tr>
<tr>
<td>Manager</td>
<td>Link for selecting an employee as manager</td>
</tr>
<tr>
<td></td>
<td>By default, the logged in user is assigned as the manager. The business role is displayed with the manager responsible.</td>
</tr>
<tr>
<td>Deputy manager</td>
<td>Link for selecting the deputy manager</td>
</tr>
<tr>
<td>Employees do not inherit</td>
<td>If set, employees are prevented from inheriting</td>
</tr>
<tr>
<td>Description</td>
<td>Field for entering a reason for the new business role.</td>
</tr>
<tr>
<td>Comment</td>
<td>Field for tips and information.</td>
</tr>
</tbody>
</table>

**Restoring deleted roles**

Another function for managing roles is restoring deleted roles. An example of a deleted role could be roles that have been sorted out during merging.

This function is also available in the views of managed organizations. Restoring a deleted role is described in the following step-by-step on the basis of a business role.

**To restore deleted roles**

1. Perform one of the following tasks.
   - Open the **Business roles** menu and **Restore a deleted role**.
   - OR -
   - Restore a lower-level role by selecting a business role in the **Business roles** menu and clicking **Restore**.

   This opens a dialog. The view **Select deleted role** is enabled and lists all the deleted objects.

   **NOTE:** You can set a date in order to limit your search for deleted roles.

2. Select the desired role and click **Next**.

   Multi-select is possible. The view **Verify** appears and lists the actions that will be run on restore.

3. You can deselect individual actions if you do not want to run them all. Click **Continue**.

4. Close the dialog.
Master data

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

Depending on your responsibilities and approvals, you can change your responsibility properties. For example, you can change the name of a department to make it easier for your staff or add managers for sharing data.

In the step-by-step, editing a responsibility is explained on the basis of business role master data. Editing options vary and depend on the selected object type.

**To edit your responsibility properties**

1. Perform one of the following tasks.
   a. Open the **Business Roles** menu and select a business role.
   b. Open the **System Roles** menu and select a system role.
   c. Open the **Departments** menu and select a department.
   d. Open the **Cost Centers** menu and select a cost center.
   e. Open the **Locations** menu and select a location.
   f. Open the **Resources** menu and select a resource.
   g. Open the **Applications** menu and select a resource.

2. Open the **Master data**.

3. Make the following changes and click **Save**.
   The setting vary and are dependent on the selected object type.

**Table 53: Business role master data**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object type</td>
<td>Field for the object type name.</td>
</tr>
<tr>
<td></td>
<td>The field’s identifier depends on the selected object type.</td>
</tr>
<tr>
<td>Short name</td>
<td>Field for a shorten name.</td>
</tr>
<tr>
<td>Internal name</td>
<td>Field for the internal name.</td>
</tr>
<tr>
<td>Role class</td>
<td>Link for selecting the role class.</td>
</tr>
<tr>
<td>Parent business</td>
<td>Link for selecting the parent business role.</td>
</tr>
<tr>
<td>role</td>
<td></td>
</tr>
<tr>
<td>Role type</td>
<td>Menu for selecting the role type.</td>
</tr>
<tr>
<td>Manager</td>
<td>Link for selecting an employee as manager.</td>
</tr>
</tbody>
</table>
### Setting | Description
---|---
By default, the logged in user is assigned as the manager. The business role is displayed with the manager responsible.

| Deputy manager | Link for selecting the deputy manager. |
| Attestors | Link for selecting the parent business role. |
| Department | Link for selecting the department. |
| Location | Link for selecting the location. |
| Role approver | Link for selecting an application role as approver. |
| Role approver (IT) | Link for selecting an application role as approver (IT). |
| Description | Field for entering a reason for the new business role. |
| Comment | Field for tips and information. |

## Adding entitlements

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

Entitlements are items to which an employee belongs or is assigned, such as groups, accounts, roles, applications, and so on. You can add entitlements to organizations or roles for which you are responsible, and have the required access. The types of entitlements available depend on the systems in use in your company. When you add an entitlement, it is treated like a request, and you must process it using your cart. There are two ways for an employee to obtain entitlements.

- By making a request which is approved.
- Indirectly, by being assigned a role or belonging to an organization that has been assigned the entitlement.

2. **NOTE:** In order to set permissions for organizations, business or system roles in the **Requests** menu, the appropriate settings have been made in the Manager.

### To add entitlements

1. Perform one of the following tasks:
   a. Open **Business Roles** and select a business role.
   b. Open the **System Roles** menu and select a system role.
c. Open **Department** and select a department.
d. Open **Cost Center** and select a cost center.
e. Open **Locations** and select a location.

2. Select **Entitlements** and click **New**.
3. Select a type of entitlement and click **Request**.

Your shopping cart appears. For more information, see *Shopping cart* on page 76.

## Deleting entitlements

In the **Entitlements** view of a responsibility you can delete entitlements in the same manner.

### To delete an entitlement

1. Perform one of the following tasks:
   a. Open **Business Roles** and select a business role.
   b. Open the **System Roles** menu and select a system role.
   c. Open **Department** and select a department.
   d. Open **Cost Center** and select a cost center.
   e. Open **Locations** and select a location.
2. Select **Entitlements** and click **Remove entitlement**.

## Splitting a role

The original idea behind splitting a role is to take assignments from role A and transfer them to role B. An example of role splitting could be, if memberships assigned to role B have less entitlements as memberships assigned to role A.

By splitting role A assigned memberships and individual entitlements of role A can be retained, moved or copied to role B.

Any combination of role types is allowed.

### To split a role

1. Perform one of the following tasks:
   - Open **Business Roles** and select a business role.
   - Open the **System Roles** menu and select a system role.
   - Open **Department** and select a department.
- Open **Cost Center** and select a cost center.
- Open **Locations** and select a location.

2. Select **Split**.
   This opens a dialog. **New role data** is shown.

3. Configure the following in **New role data** and click **Next**.
   Fields marked with * are compulsory.

### Table 54: Settings in the view "New role data"

<table>
<thead>
<tr>
<th>Role type</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Type of the new role</td>
<td>Menu for selecting a type for the new role. The following object types are available in Web Portal.</td>
</tr>
<tr>
<td>All</td>
<td>Department / Business role / Cost center / Location *</td>
<td>Field for the new role's name. A name must be entered for every role type.</td>
</tr>
<tr>
<td>All</td>
<td>Short name</td>
<td>Text box for entering a short name for the role. This is compulsory (*) for the role type 'cost center'.</td>
</tr>
<tr>
<td>Department</td>
<td>Object ID</td>
<td>Field for an object ID for the new role.</td>
</tr>
<tr>
<td>Location / business role</td>
<td>Location</td>
<td>Field for entering a location.</td>
</tr>
<tr>
<td>Business role</td>
<td>Internal name</td>
<td>Field for an internal name for the business role.</td>
</tr>
<tr>
<td>Location</td>
<td>Name</td>
<td>Field for entering the location's name.</td>
</tr>
<tr>
<td>Department / Business role / Cost center / Location</td>
<td>Manager</td>
<td>Menu for selecting a manager responsible.</td>
</tr>
<tr>
<td>Department</td>
<td>Deputy manager</td>
<td>Menu for selecting a deputy manager.</td>
</tr>
<tr>
<td>Business role</td>
<td>Role class *</td>
<td>Role class menu.</td>
</tr>
<tr>
<td>Business role / Cost center / Location *</td>
<td>Deputy manager</td>
<td>Menu for selecting a deputy manager. Employees do not inherit is also available.</td>
</tr>
<tr>
<td>Role type</td>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Department</td>
<td>Parent department / Attestor / Cost center / Role approver / Role approver (IT)</td>
<td>Menu for selecting the respective settings</td>
</tr>
<tr>
<td>Business role</td>
<td>Parent business role / Role type / Role approver / Role approver (IT)</td>
<td>Menus for selecting the respective settings</td>
</tr>
<tr>
<td>Cost center</td>
<td>Parent cost center / Attestor / Department / Role approver / Role approver (IT)</td>
<td>Menus for selecting the respective settings</td>
</tr>
<tr>
<td>Location</td>
<td>Parent location / Attestor / Department / Cost center / Role approver / Role approver (IT)</td>
<td>Menus for selecting the respective settings</td>
</tr>
<tr>
<td>All</td>
<td>Description</td>
<td>Field for more detailed description</td>
</tr>
<tr>
<td>Business role</td>
<td>Comment</td>
<td>Field for additional comments</td>
</tr>
</tbody>
</table>

After clicking **Next**, the **Splitting** view opens. The view is divided in to the sections **No change**, **Copy to new role** and **Move to new role**, which a differentiated by color.

All memberships assigned to role A are listed in **Copy to new role**. Assigned members are copied to the new role by default. This means, they are contained in role A and in role B after splitting.

However, You can copy or move these members to the new role or retain them. The following edit options are available. Edit option also apply to assigned entitlements.

**Table 55: Assignment edit options and effects on role A and role B**

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>No change / Copy to new role / Move to new role</td>
<td>Keep this assignment.</td>
<td>The entitlement / membership remains in role A.</td>
</tr>
<tr>
<td></td>
<td>Keep and copy to new role.</td>
<td>The entitlement / membership is copied to role B. It is now in role A and in role B.</td>
</tr>
<tr>
<td>Section</td>
<td>Action</td>
<td>Significance</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td>Move to the new role.</td>
<td>The entitlement / membership is moved to role B. It is now in role B but not in role A.</td>
</tr>
</tbody>
</table>

4. Configure the assigned memberships and entitlements by navigating to an object, an employee in **Copy to new role**, for example, and clicking ▼.

5. Select one of the following actions from the menu:
   - Keep this assignment.
   - Keep and copy to new role.
   - Move to the new role.

6. Click **Next**:
   - The **Verify** view is displayed and lists the actions that are set.

7. You can deselect individual actions if you do not want to run them all.

8. Click **Next**.
   - Save changes to the script. This opens **Results**.

9. Close the dialog.

**Compliance**

In the **My Responsibilities** menu, you can view the business role compliance rule violations for which you are responsible.

**To view compliance rule violations**

1. Open the **Business Roles** menu and select a business role.
2. Click **Compliance**.
   - This displays the **Compliance** view. If rule violations exist, they are listed.
   - The following information appears:

**Table 56: The "Compliance" view**

<table>
<thead>
<tr>
<th>Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission</td>
<td>Name of permissions that caused the rule violation.</td>
</tr>
<tr>
<td>Rule</td>
<td>Name of the rule that caused the rule violation.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Shows the calculated risk index.</td>
</tr>
<tr>
<td>Risk index (reduced)</td>
<td>Shows the risk index reduced by the mitigating control.</td>
</tr>
</tbody>
</table>
In the main content view, other details about the marked compliance rule violations are displayed, such as, a description and the object class.

**Compare and merge**

You can compare and merge any combination of role types. For example, you can compare the properties of a business role and a department, take the properties you want from them and merge them. This function is available in the My Responsibilities menu for your responsibilities.

![NOTE: You can only compare and merge roles that you own or you are their administrator.](image)

**To compare and merge roles**

1. Perform one of the following tasks:
   - Open Business Roles and select a business role.
   - Open the System Roles menu and select a system role.
   - Open Department and select a department.
   - Open Cost Center and select a cost center.
   - Open Locations and select a location.

2. Select Compare and merge.
   This opens a dialog. Select a comparison role.

3. Select a second role in Comparison role and merge using Assign next to Comparison role.

   ![NOTE: If a role is already selected, use Change to edit the selection.](image)

Memberships and entitlements of the selected roles containing the following information are listed:

**Table 57: Overview of the selected roles’ assignments**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>Display name of the assigned entitlement or membership, which occurs in one of the selected roles.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the entitlement or membership.</td>
</tr>
<tr>
<td>Name of the source role</td>
<td>Assignment type if the entitlement or membership. The following assignment types are available.</td>
</tr>
<tr>
<td></td>
<td>- Direct</td>
</tr>
<tr>
<td></td>
<td>- Inherited</td>
</tr>
</tbody>
</table>

One Identity Manager 8.1.1 Web Portal User Guide
Ownerships
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| requested      | • Requested  
• Dynamic  
• Not assigned  

For more detailed information about "Basics for Assigning Company Resources", see the One Identity Manager Identity Management Base Module Administration Guide.

Name of the second role | See "Name of the source role".                                                                                                                                 |
Comparison              | Name of the role with this assignment.                                                                                                                                 |

4. View the assignments of both roles and click **Merge the selected roles**.

   ! **NOTE:** Use the filter function, which is available on nearly every column, to make the list of assignments clearer. For more information, see **Filter** on page 36.

   The Verify view is active. This lists the actions that need to run to merge the roles.

5. Verify the suggested changes and enable/disable the actions, which should be either taken or not taken into account when the roles are merged.

6. Click **Next**.

   Save changes to the script. This opens the **Results** view.

7. Close the **Compare and Merge** dialog.

   If you have transferred all the properties of the second role by merging, this role is removed from the overview.

### Restoring a previous state

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

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

#### Table 58: Factors preventing roll back

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute was not changed.</td>
<td>Change is not possible without a comparative value.</td>
</tr>
<tr>
<td>Membership resulting from delegation.</td>
<td>These memberships are not reset.</td>
</tr>
</tbody>
</table>
### Table: Factor and Description

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherited membership</td>
<td>These memberships cannot be deleted.</td>
</tr>
<tr>
<td>Membership resulting from a dynamic group</td>
<td>These memberships cannot be deleted.</td>
</tr>
</tbody>
</table>

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

1. Open **Business Roles** and select a business role.
2. Select the **Status comparison** view under **History**.
3. Use ⌛ and ⏰ to set the date and time.
   
   All the attributes for this business role are displayed in a list. These include business role properties, memberships, actions, amongst others. By default, all attributes are selected.
   
   **NOTE:** If you cannot select an attribute, the check box is not set.
4. Disable the **Roll back** check box and set each attribute you want to roll back, separately.
5. Confirm with **Roll back changes**.
   
The selected attributes are displayed in the **Roll back changes** dialog. You can still change your choice by disabling enabled attributes.

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

**Table 59: Items in the menu "View Settings"

<table>
<thead>
<tr>
<th>Menu item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset view</td>
<td>Sets the view back to default after you have, for example, applied a filter.</td>
</tr>
<tr>
<td>Save current view</td>
<td>Save the current view to using with filters, for example.</td>
</tr>
<tr>
<td>Reload data</td>
<td>Reloads the data.</td>
</tr>
</tbody>
</table>

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

### Compliance reports

**Details** is available My **Responsibilities**. In this view, you can make an initial selection to obtain a thematic detail view.
- Risk indexes and entitlements
  Shows all primary and secondary assigned member of the object type or the company structure. The member's assigned entitlements and risk indexes are displayed in the same way.

- Policy violations
  Shows all current policy violations found for the object type or the company structure.

- Compliance rule violations
  Shows all the member's current rule violations found for the object type or the company structure. Here you can resolve rule violations for marked violations. For more information, see Resolving rule violations on page 128.

To view details about an object type

1. Perform one of the following tasks:
   - Open Business Roles and select a business role.
   - Open Department and select a department.
   - Open Cost Center and select a cost center.
   - Open Locations and select a location.

2. Select Compliance reports and make an initial selection to obtain a thematic detail view.

Attestations

In My Responsibilities, you can view the attestation status for your responsibilities.

In Attestations, you can switch between the following views. Which view you see depends on the selected objects type or company structure.

- Memberships
- Entitlements of members
- Permissions
- All attestation cases

For each case you can see the current status and the creation date in the detailed content view. You can run the following action or get information.

- See whether the case was approved or denied.
- Obtain detailed information about the selected attestation case from the Information, Workflow, Attestation policy and History tabs.
- As attester, you can view attestors for pending attestation cases.
- Send a reminder.
To view attestations of the desired area of responsibility

1. Perform one of the following tasks:
   - Open Business Roles and select a business role.
   - Open the System Roles menu and select a system role.
   - Open Department and select a department.
   - Open Cost Center and select a cost center.
   - Open Locations and select a location.
   - Open Resources and select a resource.
   - Open Assignment resources and select a resource.
   - Open Multi-request resources and select a resource.
   - Open Multi requestable/unsubscribable resources and select a resource.
   - Open Applications and select an application.

2. Select Attestations.

Detailed information about this topic

- Viewing details on page 103
- Attesting pending attestations on page 103
- Sending reminders on page 104

Statistics

You can view statistics for the business roles, system roles and system entitlements that you manage.

To view statistics

1. Perform one of the following tasks.
   a. Open Business Roles and select a business role.
   b. Open the System Roles menu and select a system role.
   c. Open System entitlements and select the required system entitlement.

2. Select Statistics.

Detailed information about this topic

- Discovering your statistics on the start page on page 258
- Statistics on page 258
System roles

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

Using system roles, you can group together arbitrary company resources. You can assign these system roles to employees, workdesks or roles or you can request them through the IT Shop. Employees and workdesks inherit company resources assigned to the system roles.

System roles are not dependent on the tasks the employee performs. The roles that appear on this list are roles that you are responsible for administering.

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

- View information about the system role, members and entitlements, risk assessment and rule violations, attestation cases, and usage of various role classes.
- Change the properties of a system role.
- Add members to the role.
- Add entitlements to the role.
- View statistics.

Some functions have already been described in other menus. You can find all the functions available in this menu listed under "Detailed information about this topic".

**To open the "System Roles" menu**

- Open Responsibilities | My Responsibilities and click System Roles.

**Detailed information about this topic**

- Displaying information on page 145
- New business roles on page 166
- Adding memberships on page 159
- Deleting memberships on page 160
- Compliance on page 181
- Master data on page 168
- Attestations on page 161
- Adding entitlements on page 169
- Deleting entitlements on page 170
- Splitting a role on page 170
- Viewing risk indexes on page 149
- Splitting a role on page 170
- Compare and merge on page 174
New system role

You can add new system roles in the System Roles menu. To do this, you enter the master data.

To add a new system role

1. Open System roles and click New system role.
2. Configure the following settings in New system role and click Save.

   **NOTE:** Any fields that are not marked with an asterisk (*) are optional. Optional fields can be filled in when you create the application or at a later stage.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System role</td>
<td>Field for the system role name.</td>
</tr>
<tr>
<td>Display name</td>
<td>Field for the display name.</td>
</tr>
<tr>
<td>Internal product name</td>
<td>Field for the internal product name.</td>
</tr>
<tr>
<td>System role type</td>
<td>Menu for selecting the system role type.</td>
</tr>
<tr>
<td>Service item</td>
<td>Link for selecting a new requestable product.</td>
</tr>
<tr>
<td>System role manager</td>
<td>Link for selecting a user as manager.</td>
</tr>
<tr>
<td>Comment</td>
<td>Field for tips and information.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>If set, the system role is available through the IT Shop.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>If set, the system role is available through the IT Shop.</td>
</tr>
</tbody>
</table>
Compliance

In the **My Responsibilities** menu, you can view the system role compliance rule violations for which you are responsible.

**To view compliance rule violations**

1. Open the **System Roles** menu and select a system role.
2. Click **Compliance**.
   
   This displays the **Compliance** view. If rule violations exist, they are listed.

   The following information appears:

<table>
<thead>
<tr>
<th>Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission</td>
<td>Name of permissions that caused the rule violation.</td>
</tr>
<tr>
<td>Rule</td>
<td>Name of the rule that caused the rule violation.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Shows the calculated risk index.</td>
</tr>
<tr>
<td>Risk index (reduced)</td>
<td>Shows the risk index reduced by the mitigating control.</td>
</tr>
</tbody>
</table>

In the main content view, other details about the marked compliance rule violations are displayed, such as, a description and the object class.

Departments

Departments, cost centers and locations are organizations that part of your management scope.

After you have opened the **Departments** menu, you will see a list of all the departments and sub-departments that you manage. You can run the following tasks:

- View an overview of detailed information about the organization (in a Hyper View), its members and entitlements, attestation cases, usage of the different role classes, risk analysis and historical changes to memberships and entitlements.
- Add members to the role.
- Add entitlements to the role.
- View statistics.

Some functions have already been described in other menus. You can find all the functions available in this menu listed under "Detailed information about this topic".
To open the "Departments" menu.

- Open the menu Responsibilities | My Responsibilities and click Departments.

Detailed information about this topic

- Displaying information on page 145
- Restoring deleted roles on page 240
- Master data on page 168
- Adding memberships on page 159
- Deleting memberships on page 160
- Adding entitlements on page 169
- Deleting entitlements on page 170
- Splitting a role on page 170
- Viewing risk indexes on page 149
- Splitting a role on page 170
- Compare and merge on page 174
- History on page 152
- Timeline on page 153
- Status comparison on page 154
- Comparing the status of company resources on page 182
- Usage on page 163
- Compliance reports on page 176
- Attestations on page 177
- Statistics on page 183

Comparing the status of company resources

You can compare the current status of a company resource with their status in the past in the History view. This compares attributes which have changed within a specified time period. You specify the time period yourself in the date field provided.

As well as comparing a company resource's status, you can also compare an employee's status. For more information, see Comparing an employee's status on page 156.

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

To compare the status of a company resource

1. Open Locations and select a location.
2. Select the Status comparison view under History.
3. Use \( \text{PgUp} \) and \( \text{PgDn} \) to set the date and time.

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

**Statistics**

You can view statistics for the departments that you manage.

*To view statistics*

1. Open **Departments** and select a department.
2. Select **Statistics**.

**Detailed information about this topic**

- Discovering your statistics on the start page on page 258
- Statistics on page 258

**Cost centers**

Departments, cost centers and locations are organizations that part of your management scope.

After opening **Cost centers**, you will see a list of all the cost centers and subordinate cost centers that you manage. You can run the following tasks:

- View an overview of detailed information about the organization (in a hyper view), its members and entitlements, attestation cases, usage of different role classes, risk analysis and historical changes to memberships and entitlements
- Request members
- Add entitlements
- Viewing statistics

Some functions have already been described in other menus. You can find all the functions available in this menu listed under "Detailed information about this topic".

*To manage cost centers*

- Open the **Responsibilities | My Responsibilities** menu and click **Cost centers**.

**Detailed information about this topic**

- Displaying information on page 145
- Restoring deleted roles on page 240
Statistics

You can view statistics for the cost centers that you manage.

To view statistics

1. Open Cost Center and select a cost center.
2. Select Statistics.

Detailed information about this topic

- Discovering your statistics on the start page on page 258
- Statistics on page 258

Locations

Departments, cost centers and locations are organizations that part of your management scope.

After you open Locations, you will see a list of all the locations and sub-locations that you manage. You can run the following tasks:
- View an overview of detailed information about the organization (in a Hyper View), its members and entitlements, attestation cases, usage of the different role classes, risk analysis and historical changes to memberships and entitlements.
- Add members to the role.
- Add entitlements to the role.
- View statistics.

Some functions have already been described in other menus. You can find all the functions available in this menu listed under "Detailed information about this topic".

To manage locations
- Open Responsibilities | My Responsibilities and click Locations.

Detailed information about this topic
- Restoring deleted roles on page 240
- Displaying information on page 145
- Master data on page 168
- Adding memberships on page 159
- Deleting memberships on page 160
- Adding entitlements on page 169
- Deleting entitlements on page 170
- Splitting a role on page 170
- Attestations on page 177
- Viewing risk indexes on page 149
- History on page 152
- Timeline on page 153
- Usage on page 163
- Compliance reports on page 176
- Status comparison on page 154
- Comparing the status of company resources on page 182
- Splitting a role on page 170
- Compare and merge on page 174
- Statistics on page 185

Statistics

You can view statistics for the cost centers that you manage.
To view statistics

1. Open Cost Center and select a cost center.
2. Select Statistics.

Detailed information about this topic

- Discovering your statistics on the start page on page 258
- Statistics on page 258

Application roles

Open the One Identity Manager application roles page by selecting the Responsibilities | My Responsibilities | One Identity Manager application role.

Use application roles to quickly and simply assign to employees entitlement profiles that match their tasks and functions. The One Identity Manager already supplies a number of default application roles. You can also create custom application roles to suit your own needs.

On the One Identity Manager application roles page, you can view the application roles that you own. Select an application role to view more details.

After you have selected an application role, you can view more information about it on other pages.

Table 62: Application roles

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows all the information at a glance. You can view more, interesting information by clicking on the links inside a shape. For more information, see Displaying information about application roles on page 188.</td>
</tr>
<tr>
<td>Master data</td>
<td>Shows the application role's master data and gives you the option to edit it. For more information, see Master data of application roles on page 188.</td>
</tr>
<tr>
<td>Memberships</td>
<td>Shows the employee that the application role is assigned to. You can also add members (request membership) and delete existing memberships. For more information, see Membership in application roles on page 190.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Shows an overview of entitlements assigned to the applic-</td>
</tr>
<tr>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Compliance</td>
<td>Shows compliance violations that were caused by the application role. For more information, see Compliance rule violations of application roles on page 194.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Here you can manage the current attestation cases of the application role. You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders. For more information, see Attesting application roles on page 195.</td>
</tr>
<tr>
<td>Risk</td>
<td>Shows the application role' risk index. For more information, see Risk index of application roles on page 199.</td>
</tr>
<tr>
<td>History</td>
<td>Shows all the changes made to the application role. For more information, see Application role history on page 201.</td>
</tr>
<tr>
<td>Usage</td>
<td>Shows which roles belong to members of the application role. For more information, see Role memberships of application role members on page 204.</td>
</tr>
<tr>
<td>Compliance reports</td>
<td>Shows compliance reports about the application role. For more information, see Compliance reports of application roles on page 205.</td>
</tr>
</tbody>
</table>

**Creating application roles**

You can create new application roles to suit your requirements at anytime. Use the functions described in Application roles on page 186 to assign properties to application roles (for example, memberships, entitlements).

**To create an application role**

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application
3. On the One Identity Manager application roles page, click New application role.

4. On the Create a new application role page, enter the application role’s master data. For more information, see Master data of application roles on page 188.

5. Click Save.

Related topics

- Application roles on page 186
- Master data of application roles on page 188

Displaying information about application roles

You can view a summary of all relevant information about an application role that you own, in an overview. This information is displayed as shapes.

To display an overview of an application role

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, click the application role you want to view.
4. On the <application role name>(application role), click the Overview tile.

Related topics

- Application roles on page 186

Master data of application roles

Navigate to the Master data page through Responsibilities | My Responsibilities | One Identity Manager application roles | <application role> | Master data. For more information, see Displaying and editing application role master data on page 190.

Depending on you responsibilities and entitlements, it may be possible to change the properties of application roles that you are responsible for. For example, you can change the name of an application role so that it has more meaning and is therefore, easier to user.

On the Master data page, you can find the following data and edit it.
### Table 63: Application role master data

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application role</td>
<td>Specifies the name of the application role. Use a meaningful name so that the application role can be applied or utilized in the correct context.</td>
</tr>
<tr>
<td>Internal name</td>
<td>Specify the application role's internal name.</td>
</tr>
<tr>
<td>Parent application role</td>
<td>Specifies the application role under which the application role is organized. To open the associated overview, click on the application role shown.</td>
</tr>
<tr>
<td>Manager</td>
<td>Specifies the manager responsible for the application role. To change the application role's manager, click change and select a new manager.</td>
</tr>
<tr>
<td>Deputy manager</td>
<td>Specifies the employee who deputizes for the application role. To specify or change the application role's deputy, click Assign (no deputy assigned yet) or change respectively and select a deputy.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a description for the application role. Enter a meaningful description that exactly described what the application role is used for.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies additional advice and information about the application role.</td>
</tr>
<tr>
<td>Full name</td>
<td>Shows the full name of the application role (including path).</td>
</tr>
<tr>
<td>Department</td>
<td>Specifies which department the application role belongs to. To specify or change the application role's department, click Assign (no department assigned yet) or Change and select a department.</td>
</tr>
<tr>
<td>Location</td>
<td>Specifies which location the application role belongs to. To specify or change the application role's location, click Assign (no location assigned yet) or Change and select a location.</td>
</tr>
<tr>
<td>Cost center</td>
<td>Specifies which cost center the application role belongs to. To specify or change the application role's cost center, click Assign (no cost center assigned yet) or Change and select a cost center.</td>
</tr>
</tbody>
</table>

**Related topics**

- Application roles on page 186
- Displaying and editing application role master data on page 190
Displaying and editing application role master data

Use the master data described in Master data of application roles on page 188 to show and edit application roles.

To show and edit an application role’s master data

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role you want to edit.
4. On the <application role name> (Application role) page, click the Master data tile.
5. On the Master data - <application role name> page, make any changes to the data as necessary. For more information, see Master data of application roles on page 188.
6. Click Save.

Related topics

- Application roles on page 186
- Master data of application roles on page 188

Membership in application roles

Navigate to the Memberships page through Responsibilities | My Responsibilities | One Identity Manager application roles | <application role> | Memberships. For more information, see Displaying members of application roles on page 191.

You can assign memberships to application roles by requesting membership in the application role for a specified employee. You can only request membership in application roles that you manage and for which you own the necessary entitlements.

On the Memberships page, you will see a list of memberships that are assigned to an application role managed by you.

The following tables give you an overview of the different functions of the Memberships page.

<p>| Table 64: Membership in an application role |</p>
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees</td>
<td>Shows the employee’s name.</td>
</tr>
<tr>
<td>Origin</td>
<td>Show how the employee obtained membership in the application role.</td>
</tr>
</tbody>
</table>
Table 65: Controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request memberships</td>
<td>Use this button to add employees to the application role.</td>
</tr>
<tr>
<td>Deleting memberships</td>
<td>Use this button to remove employees from the application role.</td>
</tr>
</tbody>
</table>

Related topics

- Application roles on page 186
- Displaying members of application roles. on page 191
- Adding members to application roles on page 191
- Removing members from application roles on page 192

Displaying members of application roles.

You can display members assigned to an application role at any time.

**To show members of an application role**

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role whose members you want to show.
4. On the <application role name> (Application role) page, click the Memberships tile.
   This opens the Memberships page. For more information, see Membership in application roles on page 190.

Related topics

- Application roles on page 186
- Membership in application roles on page 190
- Adding members to application roles on page 191
- Removing members from application roles on page 192

Adding members to application roles

You can assign memberships to application roles by requesting membership in the application role for a specified employee.
To request membership of an application role

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role you want to request membership for.
4. On the <application role name> (Application role) page, click the Memberships tile.
5. On the Memberships - <application role name> page, click Request memberships.
6. In the Request memberships dialog, select the employee you want to request membership for. You can select multiple employees.
7. Click Add to cart.
   This opens the My Shopping Cart page. For more information, see Making requests on page 62.

Related topics

- Application roles on page 186
- Membership in application roles on page 190
- Displaying members of application roles on page 191
- Removing members from application roles on page 192
- Making requests on page 62

Removing members from application roles

You can delete employee membership of assigned application roles.

To delete memberships of application roles

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role you want to delete the membership from.
4. On the <application role name> (Application role) page, click the Memberships tile.
5. On the Memberships - <application role name> page, check the box next to the employee whose membership you want to delete. You can select multiple employees.
6. Click Delete memberships.
Related topics

- Application roles on page 186
- Membership in application roles on page 190
- Displaying members of application roles on page 191
- Adding members to application roles on page 191

Application role entitlements

Navigate to the Entitlements page through Responsibilities | My Responsibilities | One Identity Manager application roles | <application role> | Entitlements. For more information, see Displaying entitlements of application roles on page 193.

Employees can be assigned entitlements to different objects, such as, groups, accounts, role or applications. Assigning employees to application roles avoids you having to assign entitlements separately to each employee. All entitlements of the application role are automatically assigned to all the members of the application role. For more information about application roles, see the One Identity Manager Authorization and Authentication Guide.

On the Entitlements page, you will see a list of entitlements that are assigned to an application role managed by you.

The following tables give you an overview of the different functions of the Entitlements page.

Table 66: Application role entitlements

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlement</td>
<td>Shows the entitlement’s name.</td>
</tr>
<tr>
<td>Origin</td>
<td>Shows where the entitlement originated from.</td>
</tr>
<tr>
<td>Entitlement type</td>
<td>Show the type of entitlement (subscribed reports, account definitions, resources).</td>
</tr>
</tbody>
</table>

Related topics

- Application roles on page 186
- Displaying entitlements of application roles on page 193

Displaying entitlements of application roles

You can display entitlements of an application role at any time.
To show entitlements of an application role

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application role page, in the list, select an application role to show its entitlements.
4. On the <application role name> (application role) page, click the Entitlements tile.
   This opens the Entitlements page. For more information, see Application role entitlements on page 193.

Related topics
- Application roles on page 186
- Application role entitlements on page 193

Compliance rule violations of application roles

Navigate to the Compliance page through Responsibilities | My Responsibilities | One Identity Manager application roles | <application role> | Compliance. For more information, see Displaying compliance rule violations of application roles on page 195.

On the Compliance page, you can view compliance rule violation that were caused by application roles that you manage.

The following tables give you an overview of the different functions on the Compliance page.

Table 67: Compliance violation of an application role

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlement</td>
<td>Shows the entitlement that caused the rule violation.</td>
</tr>
<tr>
<td>Rule</td>
<td>Shows the violated rule.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Shows the severity of the rule violation (meaning the calculated risk index).</td>
</tr>
<tr>
<td>Risk index (reduced)</td>
<td>Shows the risk index taking mitigating controls into account. A rule’s risk</td>
</tr>
<tr>
<td></td>
<td>index can be reduced by a significance amount after mitigating controls have</td>
</tr>
<tr>
<td></td>
<td>been applied.</td>
</tr>
<tr>
<td></td>
<td>Mitigating controls are processes that exist outside the One Identity</td>
</tr>
<tr>
<td></td>
<td>Manager solution and that reduce the risk of violation. For more information,</td>
</tr>
<tr>
<td></td>
<td>see Governance administration on page 133.</td>
</tr>
</tbody>
</table>

TIP: You can see other details of a rule violation in the detailed view.
Related topics
- Application roles on page 186
- Displaying compliance rule violations of application roles on page 195

Displaying compliance rule violations of application roles

You can display compliance rule violations of application roles at any time.

To show compliance rule violations of application roles

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application role page, in the list, select an application role to show its rule violations.
4. On the <application role name> (Application role), click the Compliance tile.
   This open the Compliance page. For more information, see Compliance rule violations of application roles on page 194.
5. (Optional) To show details, click the desired rule violation.

Related topics
- Application roles on page 186
- Compliance rule violations of application roles on page 194

Attesting application roles

Navigate to the Attestation page through Responsibilities | My Responsibilities | One Identity Manager application roles | <application role> | Attestation. For more information, see Displaying attestation cases of application roles on page 197.

Attestation helps you to ensure the correct balance between security and compliance within the company. Attestation policies define what and whom to attest. Attestation policies are run on a schedule, and generate attestation cases. For example, having a manager attest to the groups his employees belong to provides accountability if security breaches are found.

On the Attestation page, you can view and edit all the attestation cases that relate to application role.

The attestation cases are divided in to the different categories to provide a clearer overview:
- **Memberships**: Shows all the attestation cases that relate to application role members.
- **Entitlements**: Shows all the attestation cases that relate to entitlements of application role members.
- **Object attestation**: Shows all the attestation cases that relate to the selected application role.
- **All attestation cases**: Shows all the attestation cases.

The following tables give you an overview of the different functions on the **Attestation** page.

**Table 68: Application role attestation**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Show the name of the application role the attestation case relates to.</td>
</tr>
<tr>
<td>Attestation policy</td>
<td>Show that name of the attestation policy in use.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows whether an approval decision has already been made for the attestation case.</td>
</tr>
<tr>
<td>New</td>
<td>Show you whether this is a new attestation case.</td>
</tr>
<tr>
<td>Due date</td>
<td>Show the date by which an approval decision must be made for the attestation case.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Shows the importance of the attestation case.</td>
</tr>
</tbody>
</table>

**Table 69: Controls**

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View approvers for pending cases</td>
<td>Use this button to view all employees that still have to make approval decisions about attestation cases. At this point, you can also send special reminder mails to these employees.</td>
</tr>
<tr>
<td>Send reminder</td>
<td>Use this button to send a reminder email to all the employee that still have to make approval decisions about attestation cases.</td>
</tr>
<tr>
<td>Approve</td>
<td>Use this button to open the <strong>Pending attestations: One Identity Manager application roles</strong> page. At this point, you make your approval decisions about the application roles' attestation cases.</td>
</tr>
</tbody>
</table>

**Related topics**

- Application roles on page 186
- Displaying attestation cases of application roles on page 197
- Displaying attestators for pending attestation cases of application roles and sending
reminders on page 197
• Approving attestation cases of application roles. on page 198

Displaying attestation cases of application roles

You can display application role attestation cases at any time.

To show application role attestation cases
1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role whose attestation cases you want to show.
4. On the <application role name> (Application role), click the Attestation tile. This opens the Attestation page. For more information, see Attesting application roles on page 195.

Related topics
• Application roles on page 186
• Attesting application roles on page 195
• Displaying attestators for pending attestation cases of application roles and sending reminders on page 197
• Approving attestation cases of application roles. on page 198

Displaying attestators for pending attestation cases of application roles and sending reminders

You can display attestators for pending attestation cases of application roles at any time and send reminder emails.

To show attestators for pending attestation cases of application roles and send them reminder emails
1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role whose attestation cases you want to show.
4. On the <application role name> (Application role), click the Attestation tile.
5. (Optional) Depending which attestation case you want to display, change to the
corresponding tab.

6. Click View approvers for pending cases.

7. In the Send reminder mail dialog, click in the Send reminder in the row of the employee you want to send the reminder to.

To send reminder emails

1. Run the previous steps 1 - 5.
2. On the <application role name> (Application role) page, click Send reminder.
3. In the Send reminder mail dialog, in the custom message field, enter a message for the attester.
4. Click OK.

Related topics

- Application roles on page 186
- Attesting application roles on page 195
- Displaying attestation cases of application roles on page 197
- Approving attestation cases of application roles. on page 198

Approving attestation cases of application roles.

You can make approval decisions about attestation cases of application roles.

To grant or deny approval to attestation cases of application roles.

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role whose attestation cases you want to show.
4. On the <application role name> (Application role), click the Attestation tile.
5. Select Approve.
6. On the Pending attestations: One Identity Manager application roles page, click the application role you want to approve.
7. On the Pending attestations: <application role name> page, perform one of the following actions:
   a. Grant approval for the case by clicking ☑ Approve next to the attestation case.
   b. You deny approval by clicking ☒ Deny next to the attestation case.
8. Click Next.
9. (Optional) On the **Pending attestations** page, perform one of the following actions:
   - In the **Reason for approvals** field, enter a reason for your approval decision.
     
     **NOTE:** If you have made several approval decisions, the reason you enter here applies to them all.
   - In the **Standard reason** field, select a predefined reason.
     
     **NOTE:** If you have made several approval decisions, the reason you enter or select here applies to them all.
     
     **NOTE:** You have the option of selecting a predefined text for all cases still to be approved using the **Standard reason** menu. Standard reasons are displayed in the approval history and in the case details. For more detailed information about default reasons, see the *One Identity Manager Attestation Administration Guide*.
   - If you have made several approval decisions and want to provide separate reasons for each, click **Enter a reason.** in the list next to the approval, enter a reason in the **Approval reasons** field or select a **Standard reason** from the list of reason and click **Close**.

10. Click **Save**.

11. In the **Pending attestation cases** dialog, confirm the prompt with **Yes**.

12. If the attestation policy requires multi-factor authentication, you are prompted to enter a security code. It may take a few minutes for the prompt to be displayed. Perform one of the following tasks:
   - Click **Authenticate with Starling 2FA app.**
   - Click **Send SMS** or **Phone call** and enter the security code. Click **Next**.

For more information, see *Requesting a Starling 2FA token* on page 79.

**Related topics**

- **Application roles** on page 186
- **Attesting application roles** on page 195
- **Displaying attestation cases of application roles** on page 197
- **Displaying attestators for pending attestation cases of application roles and sending reminders** on page 197

**Risk index of application roles**

Navigate to the **Risk** page through **Responsibilities** | **My Responsibilities** | **One Identity Manager application roles** | <application role> | **Risk**. For more information, see *Displaying risk indexes of application roles* on page 200.

On the **Risk** page, you can view risk indexes of the application roles you manage. For more information about risk assessment, see *Risk assessment* on page 135.
The following tables give you an overview of the different functions on the Risk page.

**Table 70: Controls**

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calculated risk</td>
<td>Use this button to view the calculated risk of the application role.</td>
</tr>
<tr>
<td>View risk</td>
<td>You can view which attributes and assignments of the application role</td>
</tr>
<tr>
<td>functions</td>
<td>contribute to the risk index calculation.</td>
</tr>
</tbody>
</table>

**Related topics**

- Application roles on page 186
- Displaying risk indexes of application roles on page 200
- Risk assessment on page 135

**Displaying risk indexes of application roles**

You can view the risk index of an application role at any time.

*To show the risk index of an application role.*

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role whose risk index you want to show.
4. On the `<application role name>` (Application role), click the Risk tile.
   - This opens the Risk page. For more information, see Risk index of application roles on page 199.
5. (Optional) To display the application role's attributes and assignments that contribute to calculating the risk index, click View risk functions.

**Related topics**

- Application roles on page 186
- Risk index of application roles on page 199
- Risk assessment on page 135
Application role history

Navigate to the History page through Responsibilities | My Responsibilities | One Identity Manager application roles | <application role> | History. For more information, see Displaying application role history on page 202.

On the History page, you can view all modifications to the application roles that you manage. The information is divided out on to three tabs:

- **Events**: Shows all the events, which affect an application role, on either a timeline or in a table.
- **Status overview**: Shows a list of modified properties with the validity time period and corresponding date of change.
- **Status comparison**: Shows a comparison between the current and the selected point in time.

The following tables give you an overview of the different functions on the History page.

### Table 71: History of an application role

<table>
<thead>
<tr>
<th>Tabs</th>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Events</strong></td>
<td>Change type</td>
<td>Shows the type of change.</td>
</tr>
<tr>
<td></td>
<td>Property</td>
<td>Shows the type of the modified object.</td>
</tr>
<tr>
<td></td>
<td>Display</td>
<td>Shows the name of the modified object.</td>
</tr>
<tr>
<td></td>
<td>Date</td>
<td>Shows the date the change was made.</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>Shows the user that made the change.</td>
</tr>
<tr>
<td><strong>Status overview</strong></td>
<td>Display</td>
<td>Shows the type of change.</td>
</tr>
<tr>
<td></td>
<td>Property</td>
<td>Shows the type of the modified object.</td>
</tr>
<tr>
<td></td>
<td>Value</td>
<td>Shows the name of the modified object.</td>
</tr>
<tr>
<td></td>
<td>Run started</td>
<td>Shows the start date of the validity period.</td>
</tr>
<tr>
<td></td>
<td>End</td>
<td>Shows the end date of the validity period.</td>
</tr>
<tr>
<td>Tabs</td>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Status comparison</td>
<td>Modified</td>
<td>Show whether the change took place or not.</td>
</tr>
<tr>
<td></td>
<td>Change type</td>
<td>Shows the type of change.</td>
</tr>
<tr>
<td></td>
<td>Object type</td>
<td>Shows the type of the modified object.</td>
</tr>
<tr>
<td></td>
<td>Property</td>
<td>Shows the name of the modified object.</td>
</tr>
<tr>
<td></td>
<td>Historical value</td>
<td>Shows the value be the modification.</td>
</tr>
<tr>
<td></td>
<td>Current value</td>
<td>Show the current value.</td>
</tr>
</tbody>
</table>

**Related topics**

- Application roles on page 186
- Displaying application role history on page 202

**Displaying application role history**

You can view the history of an application role at any time.

**To show the history of an application role**

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role whose risk index you want to show.
4. On the `<application role name>` (Application role), click the History tile.
   - This opens the History page and displays the timeline. For more information, see Application role history on page 201.

   ⚠️ **TIP**: To navigate along the timeline, click in the pane and move the mouse left or right whilst holding down the left button.
   - To zoom in or out, turn the mouse wheel.
To filter the timeline by a particular event

1. On the History page, click Filter by... and select one of the following entries:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Searches for events or actions associated with the given name. Employees with entitlements and ownerships create changes, such as adding or removing properties. You can view these actions on the timeline.</td>
</tr>
<tr>
<td>Change type</td>
<td>Lists all changes types, which can be selected for displaying in the timeline. Multi-select is possible.</td>
</tr>
<tr>
<td>Date</td>
<td>List all actions and events for the selected date.</td>
</tr>
<tr>
<td>Property</td>
<td>Lists all properties, which can be selected for displaying in the timeline. Multi-select is possible.</td>
</tr>
<tr>
<td>Display</td>
<td>Searches for all text data matching the given search term. The following settings are available.</td>
</tr>
<tr>
<td></td>
<td>- All words</td>
</tr>
<tr>
<td></td>
<td>- Starts with...</td>
</tr>
<tr>
<td></td>
<td>- Ends with...</td>
</tr>
<tr>
<td></td>
<td>- One or more words</td>
</tr>
</tbody>
</table>

2. Apply the selected filter with Filter on.

To display the history as a table

- On the History page, click Switch to table view.

  TIP: If you want to switch back to the timeline view, click Switch to timeline view.

To display a list of modified properties with their validity period and dates when they were changed.

- On the History page, switch to the Status overview tab.

To compare the current status of an object with a date in the past

1. On the History page, switch to the Status comparison tab.
2. On the Status comparison, check the box and enter a date to compare.
Related topics

- Application roles on page 186
- Application role history on page 201

Role memberships of application role members

Navigate to the Usage page through Responsibilities | My Responsibilities | One Identity Manager application roles | <application role> | Usage. For more information, see Displaying role memberships on page 204.

On the Usage page, you can view which roles belongs to the members of application roles that you manage. The information is displayed as a hierarchical chart, which shows you more about the role inheritance.

The following tables give you an overview of the different functions on the Usage page.

Table 72: Controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role classes</td>
<td>Use this list of roles to select what you want to view.</td>
</tr>
<tr>
<td>More information</td>
<td>Use this button to show the legend that explains the content of the overview.</td>
</tr>
</tbody>
</table>

Displaying role memberships

You can display which role belong to members of an application role.

To show usage of application roles

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the My Responsibilities page, click the One Identity Manager application roles tile.
3. On the One Identity Manager application roles page, in the list, select the application role whose usage you want to show.
4. On the <application role name> (Application role), click the Usage tile.
5. On the Usage - <application role name> (Application role), in the Role classes list, select the main category of the role you want to show.
This displays the role class overview.

**TIP:** To show the legend that explains the content of the overview, click **More information**.

6. (Optional) In the overview, click on an object to show the sub-objects.

**Related topics**

- Application roles on page 186
- Role memberships of application role members on page 204

**Compliance reports of application roles**

Navigate to the **Compliance reports** page through **Responsibilities | My Responsibilities | One Identity Manager application roles | <application role> | Compliance reports**. For more information, see **Displaying compliance reports of application roles** on page 206.

On the **Compliance reports** page, you can view compliance reports of application roles that you manage. The data is divided between three menus:

- **Policy violations**: Shows all current rule violations that have been caused by the application role.
- **Compliance rule violations**: Shows all the current rule violations of application role members.
  
  **TIP:** For more information about resolving rule violations, see **Resolving rule violations** on page 128.
- **Members: Risk indexes and entitlements**: Shows all primary and secondary assigned members of the application role. The member's assigned entitlements and risk indexes are displayed in the same way.

Use the **View** list to open the menus.

The following tables give you an overview of the different functions on the **Compliance reports** page.

**Table 73: Compliance reports of an application role**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy violations</td>
<td>Violating object</td>
<td>Show which object caused the rule violation.</td>
</tr>
<tr>
<td></td>
<td>Policy</td>
<td>Show the policy that was violated.</td>
</tr>
<tr>
<td>Menu</td>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Compliance rule violations</td>
<td>Status</td>
<td>Show the status of the rule policy.</td>
</tr>
<tr>
<td>Compliance rule violations</td>
<td>Employee</td>
<td>Shows the employee who caused the violation.</td>
</tr>
<tr>
<td>Compliance rule violations</td>
<td>Rule violation</td>
<td>Shows the violated rule.</td>
</tr>
<tr>
<td>Compliance rule violations</td>
<td>Approval state</td>
<td>Shows how or whether approval is granted to the rule violation.</td>
</tr>
<tr>
<td>Compliance rule violations</td>
<td>Risk index (reduced)</td>
<td>Shows the risk index taking mitigating controls into account. A rule’s risk index can be reduced by a significance amount after mitigating controls have been applied. Mitigating controls are processes that exist outside the One Identity Manager solution and that reduce the risk of violation. For more information, see Governance administration on page 133.</td>
</tr>
</tbody>
</table>

**Members: Risk indexes and entitlements**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>Show the employees who are assigned to the application role.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>Shows the severity of the rule violation (meaning the calculated risk index). The higher this value is, the higher the risk for the employee.</td>
</tr>
<tr>
<td>Assigned permissions</td>
<td>Shows all the entitlements assigned to this employee.</td>
</tr>
</tbody>
</table>

**Related topics**

- Application roles on page 186
- Displaying compliance reports of application roles on page 206
- Resolving rule violations on page 128
- Governance administration on page 133

**Displaying compliance reports of application roles**

You can view an application role's compliance reports at any time.
To displaying compliance reports of application roles

1. In the menu bar, click Responsibilities | My Responsibilities.

2. On the My Responsibilities page, click the One Identity Manager application roles tile.

3. On the One Identity Manager application roles page, in the list, select the application role whose compliance reports you want to show.

4. On the <application role name> (Application role), click the Compliance reports tile.

5. On the Compliance reports page, in the View list, select one of the following entries:
   - **Policy violations**: Shows all current rule violations that have been caused by the application role.
   - **Compliance rule violations**: Shows all the current rule violations of application role members.
   - **Members: Risk indexes and entitlements**: Shows all primary and secondary assigned members of the object type or the company structure. The member's assigned entitlements and risk indexes are displayed in the same way.

   **TIP**: For more information, see Resolving rule violations on page 128.

   - **Members**: Shows all primary and secondary assigned members of the object type or the company structure. The member's assigned entitlements and risk indexes are displayed in the same way.

   **TIP**: For more information, see Compliance reports of application roles on page 205.

Related topics

- Application roles on page 186
- Compliance reports of application roles on page 205
- Resolving rule violations on page 128

Resources

In the Resources menu, you can view the resources that you manage. An employee can own resources once and they can only be requested by them once. After being approved, they remain assigned until they are unsubscribed. You can request them again at a later point. Examples for resource are telephones or company cars.

You can execute the following actions for each resource:

- View overview pages about a resource (Hyper View) with all the required details, like assigned service items, memberships, and their usage.
- Change resource properties.
- Add new resources and applications.
- Add employees to a resource.
Some functions have already been described in other menus. You can find all the functions available in this menu listed under "Detailed information about this topic".

**To open the "Resources" menu**

- Open the menu Responsibilities | My Responsibilities and click Resources.

**Detailed information about this topic**

- Displaying information on page 145
- New resources on page 208
- Master data on page 168
- Adding memberships on page 159
- Deleting memberships on page 160
- Attestations on page 177
- Usage on page 163

**New resources**

In the Resources menu, you can add new resources. To do this, you enter the master data.

**To add a new resource**

1. Open Resources and click New resource.
2. Configure the following settings for the new resource and click Save.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Field for naming the resource.</td>
</tr>
<tr>
<td>Resource type</td>
<td>Link for selecting the resource type.</td>
</tr>
<tr>
<td>Description</td>
<td>Field for entering a reason for the new resource.</td>
</tr>
<tr>
<td>IT Shop</td>
<td>If set, the resource is available through the Web Portal.</td>
</tr>
<tr>
<td></td>
<td>The resource can still be assigned directly to employees and hierarchical roles.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>If set, the resource is only available through the Web Portal.</td>
</tr>
<tr>
<td></td>
<td>The resource may not be assigned directly to hierarchical roles.</td>
</tr>
<tr>
<td>Service item</td>
<td>Link for selecting a new requestable product.</td>
</tr>
</tbody>
</table>
Assignment resources

On the Assignment resources page, you can view all the assignment resources that you manage. Use assignment resources to request hierarchical roles, such as departments or business roles and assign them to employees, devices and workdesks. This means, for example, you can limit assignment resources to a certain business role, which makes it unnecessary to select the business role additionally when you request an assignment resource. It is automatically a part of the assignment request. Assignment resources are available for requesting in the shop "Identity & Access Lifecycle". For more information about assignment resources, see the One Identity Manager Business Roles Administration Guide and One Identity Manager IT Shop Administration Guide.

You can execute the following actions for each resource:

- View overview pages about a resource (hyper view) with all the required details, like assigned service items, memberships and their usage.
- Change the assignment resource properties

Some functions have already been described in other menus. You can find all the functions available in this menu listed under "Detailed information about this topic".

To display the assignment resources that you manage

1. In the menu bar, click Responsibilities | My Responsibilities.
2. On the Auditing page, click the Assignment resources tile.

TIP: You can view all assignment resources or assignment resources assigned to other employees. For more information, see Assignment resources on page 237.

Detailed information about this topic

- Displaying information on page 145
- Adding memberships on page 159
- Deleting memberships on page 160
- Attestations on page 177
- Usage on page 163

Multi-request resources

In My Responsibilities, you can see the resources that you have requested in IT Shop more than once. Multi-requestable resources are automatically unsubscribed after the request has been granted approval. These resources are not explicitly assigned to the employee. Examples include consumables such as pens or printing paper.
To open "Multi-requestable/unsubscribable resources"

- Open Responsibilities | My Responsibilities and click Multi-request resources.

Detailed information about this topic

- Displaying information on page 145
- Adding memberships on page 159
- Deleting memberships on page 160
- Attestations on page 177
- Usage on page 163

Multi-requestable/unsubscribable resources

In the menu, Multi-requestable/unsubscribable Resources, you can view all the resources that you manage. You can request multi-requestable/unsubscribable resources more than once in the IT Shop. These resources must, however, be returned explicitly when they are no longer required. They are assigned to employees after approval has been granted and they remain assigned until the request is canceled. An example of multi-requestable/unsubscribable resources would be printers or monitors.

You can execute the following actions for each resource:

- View overview pages about a resource (Hyper View) with all the required details, such as assigned service items, memberships, and their usage.
- Change resource properties.
- Add new resources and applications.
- Add employees to a resource.

Some functions have already been described in other menus. You can find all the functions available in this menu listed under "Detailed information about this topic".

To manage multi-requestable/unsubscribable resources

- Open the Responsibilities | My Responsibilities and click Multi-requestable/unsubscribable resources.

Detailed information about this topic

- Displaying information on page 145
- Adding memberships on page 159
- Deleting memberships on page 160
- Attestations on page 177
- Usage on page 163
Applications

In Applications, you can view all the applications you are responsible for. You can assign applications directly or indirectly to employees. Indirect assignment is carried out by assigning employees and applications to company structures, such as departments, cost centers, locations, or business roles. Assigned applications might be internet software, address management, mail, or text handling, for example.

Detailed information about this topic

- Adding new applications on page 211
- Displaying information on page 145
- Master data on page 168
- Adding memberships on page 159
- Deleting memberships on page 160
- Attestations on page 177
- Usage on page 163

Adding new applications

In Applications, you can add new applications. To do this, you enter the master data.

To add a new application

1. Open Applications and click New application.
2. Configure the following settings for the new application and click Save.

   NOTE: Any fields that are not marked with an asterisk (*) are optional. Optional fields can be filled in when you create the application or at a later stage.

Table 75: Settings and data for new applications

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>Field for an application name. Enter the name of the application.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the application.</td>
</tr>
<tr>
<td>Language</td>
<td>Language settings. The selected language is used for the application.</td>
</tr>
<tr>
<td></td>
<td>Use Assign to select the language.</td>
</tr>
</tbody>
</table>
Setting | Description
--- | ---
Service item | If you assign a service item to the application, the application usage can be booked internally. Make a new service item using **Create a new service item.** Enter the data about the service category and product owner for the new service item in **New service item.**
Internal product name | Application name used internally.
Website | The application’s website.
Link to documentation | Link to the application’s documentation.
Description | Field for additional explanations.
Comment | Field for additional explanations.
IT Shop | If this option is set, the application is available in the IT Shop.
Only for use in IT Shop | This can only be changed if the **IT Shop** option is set. If this option is set, the application is only available in the IT Shop.
Deactivated | If set, a disabled application is added.

**Devices**

You can view your devices in the **Devices** menu and assign new devices to yourself. If you have sufficient permissions, you can add new devices or make changes to the device assignments for your staff.

**To open the "Devices" menu**

- Open the menu **Responsibilities | My Responsibilities** and click **Devices**.

**Detailed information about this topic**

- Displaying information on page 145
- Adding new devices on page 213
- Editing master data on page 215
Adding new devices

You can assign devices to employee in Devices.

To add a new device

1. Open the menu Devices and click Add a new device.
2. In the Add a new device view, select the device type from the Device type list.
3. Assign the required model in Device model and click Next.

This opens Add a new device with more form fields. The type of data input required depends on the type of device. Enter the following data.

Table 76: Device master data

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used by</td>
<td>Select a future user for the device</td>
</tr>
<tr>
<td></td>
<td>The current user is selected by default.</td>
</tr>
<tr>
<td></td>
<td>Use Change to select another user from the list.</td>
</tr>
<tr>
<td></td>
<td>You can only select another user if you own the required permissions or you have your own staff.</td>
</tr>
<tr>
<td>Device model</td>
<td>Select a device model</td>
</tr>
<tr>
<td></td>
<td>You have already entered this in the 3rd step of these step-by-step instructions. Use Change to select another device model.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Select a device manufacturer</td>
</tr>
<tr>
<td></td>
<td>Use Assign to select a manufacturer from the list.</td>
</tr>
<tr>
<td>Device ID</td>
<td>Identifier for the device</td>
</tr>
<tr>
<td></td>
<td>Enter the device’s identifier if you know it.</td>
</tr>
<tr>
<td>Device status</td>
<td>Select device status</td>
</tr>
<tr>
<td></td>
<td>Use Assign to select the device's status.</td>
</tr>
<tr>
<td>Enabling</td>
<td>Data field for the activation time and date</td>
</tr>
<tr>
<td></td>
<td>Enable the checkbox and enter the activation time and date in the data field.</td>
</tr>
<tr>
<td>Deactivation</td>
<td>Data field for the deactivation time and date</td>
</tr>
<tr>
<td></td>
<td>Enable the checkbox and enter the deactivation time and date.</td>
</tr>
<tr>
<td>Asset number</td>
<td>Asset number input</td>
</tr>
<tr>
<td></td>
<td>Enter the asset number if you know it.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>Company owned</td>
<td>Checkbox to define the device as belonging to the company</td>
</tr>
<tr>
<td></td>
<td>Enable the checkbox to define the device as company property.</td>
</tr>
<tr>
<td>Location description</td>
<td>Location input</td>
</tr>
<tr>
<td></td>
<td>Enter the location where the device will be used.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Serial number input</td>
</tr>
<tr>
<td></td>
<td>Enter the device's serial number, if known.</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address input</td>
</tr>
<tr>
<td></td>
<td>Enter the device's MAC address.</td>
</tr>
<tr>
<td>Storage capacity [GB] / RAM [MB]</td>
<td>Storage capacity / RAM information input</td>
</tr>
<tr>
<td></td>
<td>Enter the device’s storage capacity / RAM.</td>
</tr>
<tr>
<td>BIOS version</td>
<td>BIOS version input</td>
</tr>
<tr>
<td></td>
<td>Enter the BIOS version if this device is a PC.</td>
</tr>
<tr>
<td>Operating system</td>
<td>Name of the operating system input</td>
</tr>
<tr>
<td></td>
<td>Enter the name of the operating system used by the device.</td>
</tr>
<tr>
<td>Operating system version</td>
<td>Operation system’s version input</td>
</tr>
<tr>
<td></td>
<td>Enter the version number of the operating system currently installed on the device.</td>
</tr>
<tr>
<td>Carrier (* only displayed for mobile phones or tablets)</td>
<td>Name of the carrier input</td>
</tr>
<tr>
<td></td>
<td>Enter the name of the carrier to be used with the device.</td>
</tr>
<tr>
<td>IMEI (* only displayed for mobile phones or tablets)</td>
<td>International Mobile Station Equipment Identity (IMEI) input</td>
</tr>
<tr>
<td></td>
<td>Enter the IMEI if the device is a mobile phone.</td>
</tr>
<tr>
<td>ICCID (* only displayed for mobile phones or tablets)</td>
<td>Integrated Circuit Card ID (ICCID) input</td>
</tr>
<tr>
<td></td>
<td>Enter the ICCID number (SIM card number) if the device is a mobile phone.</td>
</tr>
<tr>
<td>Phone (* only displayed for mobile phones)</td>
<td>Telephone number input</td>
</tr>
<tr>
<td></td>
<td>Enter the telephone number, if this device is a mobile phone.</td>
</tr>
<tr>
<td>PC / Server / VM host / VM client</td>
<td>Checkbox for enabling</td>
</tr>
</tbody>
</table>
### Editing master data

In the Devices menu, you can edit the master data of devices you already manage. You could assign a tablet to another employee, for example, or change the device’s status, the manufacturer or the device model. You can also add any missing information in the master data.

**To edit the master data of a managed device**

1. Click the device to edit in Devices.
2. Set the following master data.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used by</td>
<td>Select a future user for the device&lt;br&gt;The current user is selected by default.&lt;br&gt;Use Change to select another user from the list.&lt;br&gt;You can only select another user if you own the required permissions or you have your own staff.</td>
</tr>
<tr>
<td>Device model</td>
<td>Select a device model&lt;br&gt;You have already entered this in the 3rd step of these step-by-step instructions. Use Change to select another device model.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Select a device manufacturer&lt;br&gt;Use Assign to select a manufacturer from the list.</td>
</tr>
<tr>
<td>Device ID</td>
<td>Identifier for the device&lt;br&gt;Enter the device's identifier if you know it.</td>
</tr>
</tbody>
</table>

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

4. Save the changes.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device status</td>
<td>Select device status</td>
</tr>
<tr>
<td></td>
<td>Use <strong>Assign</strong> to select the device's status.</td>
</tr>
<tr>
<td>Enabling</td>
<td>Data field for the activation time and date</td>
</tr>
<tr>
<td></td>
<td>Enable the checkbox and enter the activation time and date in the data field.</td>
</tr>
<tr>
<td>Deactivation</td>
<td>Data field for the deactivation time and date</td>
</tr>
<tr>
<td></td>
<td>Enable the checkbox and enter the deactivation time and date.</td>
</tr>
<tr>
<td>Asset number</td>
<td>Asset number input</td>
</tr>
<tr>
<td></td>
<td>Enter the asset number if you know it.</td>
</tr>
<tr>
<td>Company owned</td>
<td>Checkbox to define the device as belonging to the company</td>
</tr>
<tr>
<td></td>
<td>Enable the checkbox to define the device as company property.</td>
</tr>
<tr>
<td>Location description</td>
<td>Location input</td>
</tr>
<tr>
<td></td>
<td>Enter the location where the device will be used.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Serial number input</td>
</tr>
<tr>
<td></td>
<td>Enter the device's serial number, if known.</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address input</td>
</tr>
<tr>
<td></td>
<td>Enter the device's MAC address.</td>
</tr>
<tr>
<td>Storage capacity [GB] / RAM [MB]</td>
<td>Storage capacity / RAM information input</td>
</tr>
<tr>
<td></td>
<td>Enter the device's storage capacity / RAM.</td>
</tr>
<tr>
<td>BIOS version</td>
<td>BIOS version input</td>
</tr>
<tr>
<td></td>
<td>Enter the BIOS version if this device is a PC.</td>
</tr>
<tr>
<td>Operating system</td>
<td>Name of the operating system input</td>
</tr>
<tr>
<td></td>
<td>Enter the name of the operating system used by the device.</td>
</tr>
<tr>
<td>Operating system version</td>
<td>Operation system's version input</td>
</tr>
<tr>
<td></td>
<td>Enter the version number of the operating system currently installed on the device.</td>
</tr>
<tr>
<td>Carrier</td>
<td>Name of the carrier input</td>
</tr>
<tr>
<td>(   * only displayed for mobile phones or tablets)</td>
<td>Enter the name of the carrier to be used with the device.</td>
</tr>
</tbody>
</table>
### Adding tags for service items

You can add tags if you are the product owner and the service item can be requested in the IT Shop. Tags help the requester to find the service item for a request, faster. You can search within the Request menu or with the global search in the Web Portal.

Tags can be added in the Manager as well as in the Web Portal. Add tags in the Web Portal as a product owner. For more detailed information, see the One Identity Manager IT Shop Administration Guide.

#### To add a tag for a service item

1. Open **My Responsibilities** and click a responsibility, for example, **System entitlements**.
2. Select **Overview** and click the object name in the **Service item** shape.
3. Select **Tags** on the object’s page and click **New tag**.
4. Enter the new tag and other information about the tag in the **Create a new tag**.
5. Click **Save**.

You can add more tags for the object.
Task delegation

Delegation is a submenu of Responsibilities. Here you can delegate your responsibilities and view your delegation history. These actions can be called up over tiles.

Detailed information about this topic

- Adding new delegations on page 218
- Deleting delegations on page 219

Delegation

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

In the Delegations menu, you can cancel and delete delegations. All your delegations are listed here. You can cancel and delete approved delegations. These delegations are marked with the Approved status.

You can only delete delegations which are not approved. Unapproved delegations have the status Request or Assigned. The delegation status is displayed in the detailed content view.

You can see the current status and validity, amongst other things, for every single delegation in the detailed content view. You can run the following action or get information.

- You obtain detailed information about the selected delegation on the Delegation and Employee tabs.
- The Details on the Delegation tab provide you with an extended version of the delegation information that is divided between the Information, Workflow and Compliance tabs.

To open the "Delegation" menu.

- Open the menu Responsibilities | Delegation and click Delegation.

Adding new delegations

You can add new delegations in the Delegation menu.

To add a new delegation

1. Open Delegation and click New delegation.
   This opens the wizard for delegating role memberships and responsibilities. The Select a recipient view is selected.
2. Select a recipient of the delegation with Assign and click Next.
3. Mark the role you want to delegate in Select roles and click Next.

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

   Enter additional information is now visible.
4. Configure the following settings in Enter additional information and click Save.

   Table 78: Additional information for delegation

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid from</td>
<td>Start date and time of the delegation.</td>
</tr>
<tr>
<td>Valid until</td>
<td>Expiry date and time of the delegation.</td>
</tr>
<tr>
<td>Notify me if the recipient of the delegation makes a decision.</td>
<td>If the option is set, you receive a message in this case.</td>
</tr>
<tr>
<td>The recipient can delegate this role</td>
<td>If the option is set, the recipient of the delegation can delegate the role to someone else.</td>
</tr>
<tr>
<td>Reason</td>
<td>Field for entering a reason for delegating.</td>
</tr>
<tr>
<td>Priority</td>
<td>Menu for selecting a priority. The following priorities are available:</td>
</tr>
<tr>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td></td>
<td>• High</td>
</tr>
<tr>
<td></td>
<td>• Medium</td>
</tr>
<tr>
<td></td>
<td>• Low</td>
</tr>
</tbody>
</table>

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

Deleting delegations

You delegations are displayed in the Delegation menu. You can limit the number of delegations displayed by filtering them. You can apply a filter to the column Type, for example. Here you can filter the assignment type by the following:
- Employee manager
- Role manager
- Business owner
- Membership

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

**To delete one, several, all visible or your own delegations**

1. Open Delegation.
2. Use a filter and then mark the item you want in the result list.
3. Perform one of the following tasks.

<table>
<thead>
<tr>
<th>Table 79: Ways of deleting delegations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Delete a single delegation</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Delete all visible delegations</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Delete your own delegations</td>
</tr>
</tbody>
</table>

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

**Delegation history**

In the delegation history, you can view all the delegations that you have been issued or have issued yourself.

You will see the name, type, validity of the delegation and to whom it was delegated in the list of delegations.
For each delegation, you can obtain more information on the Information, Workflow, Compliance and Entitlements tabs in the detailed content view.

Related topics
- Displaying delegation history

Displaying delegation history

To show delegation history
1. In the header, select Responsibilities | Delegation.
3. On the Delegation history page, filter which delegation are shown:
   - **Valid from**: All delegations that are valid as from this time on or from a time point within this period are taken into account.
   - **Valid until**: All delegations that are valid up to this time or up to a time point within this period are taken into account.
4. (Optional) Click Advanced search and do one of the following:
   a. Click Assign next to the Delegator field.
   b. In the Employee dialog, click on the employee who issued the delegation.
   c. On the Delegation history page, click Assign next to the Delegation recipient field.
   d. In the Employee dialog, click on the employee whom the delegation was issued to.
   e. To show additional delegations that are not in effect, check the Show never assigned delegations box.
5. Click Search.

For each delegation, you can obtain more information on Information, Workflow, Compliance, and Entitlements.

**Examples**

You want to show delegations that are valid as from 01/01/2019:
1. Uncheck the all checkboxes apart from the one next to **Valid from**.
2. In the field next to **Valid from**, select the date **01/01/2019**.
3. Click **Search**.

You want to show delegations that are valid from 01/01/2019 until 02/01/2019:
1. Uncheck the all checkboxes apart from the one next to Valid from and the first Valid until.
2. In the field next to Valid from, select the date 01/01/2019.
3. In the field next to Valid until, select the date 02/01/2019.
4. Click Search.

You want to show all delegations whose valid from date is between 01/01/2019 and 03/01/2019:
1. Uncheck the all checkboxes apart from the first and the second one next to Valid from.
2. In the first field next to Valid from, select the date 01/01/2019.
3. In the second field next to Valid from, select the date 03/01/2019.
4. Click Search.

Related topics
- Delegation history

**Ownerships**

**Ownerships** is a submenu of Responsibilities. Here, you can assign business objects to owners or request responsibility for a group.

**NOTE:** In the Responsibilities menu, either Assign ownership or Claim responsibility is visible. Which of the menus is displayed, depends on the system settings.

**Detailed information about this topic**
- Assigning owners on page 222
- Claim ownership on page 224

**Assigning owners**

In the Assign Ownership menu, you can assign an owner to devices and system entitlements, which do not have owners assigned. A wizard is available to help you make the assignments.

**IMPORTANT:** Before you can use this function, you need the "Device ownership attestation" or "System entitlement ownership attestation" attestation policy.
NOTE: In the Responsibilities menu, either Assign ownership or Claim responsibility is visible. Which of the menus is displayed, depends on the system settings.

Detailed information about this topic

- Assigning owners to devices on page 223
- Assigning system entitlements owners on page 223

Assigning owners to devices

In Assign Ownership, you can assign an owner to a device.

NOTE: In the Responsibilities menu, either Assign ownership or Claim responsibility is visible. Which of the menus is displayed, depends on the system settings.

To assign an owner to a device

1. Open Assign ownership and click Device.
   
   This opens a wizard. The view Select a device is active.

2. Click Assign next to Device and select a device from the list.
   
   This selects the device and displays details about it, for example, device model, workdesk, and cost center.

3. Click Next and select one of the options from Select the new owner.
   
   a. Select one of the calculated possible owners.

   b. Select another owner.

   For these settings, select an employee from the displayed list.

4. Click Next and then Close in Results.

Assigning system entitlements owners

In Assign Ownership, you can assign an owner to a system entitlement.

To assign system entitlements to an owner

1. Open Assign ownership and click System entitlement.
   
   This opens a wizard. Select a system entitlement is active.

2. Click Assign next to System entitlement and select a group from the list.
   
   This selects the group and displays details about it, for example, group type or target system.
3. Click **Next** and select one of the options from **Select the new owner**.
   a. Select one of the calculated possible owners.
      In this case, you do not have to change any other settings.
   b. Select another owner.
      In this case, select an employee from the displayed list.
4. Click **Next** and then **Close** in **Results**.

**Claim ownership**

You can claim ownership of a group in **Claim Ownership** under the **My Responsibilities** menu.

The groups available for selection, do not have any managers. Authorized users can take on responsibility for these groups. If you claim ownership for a group, you are accountable for the interests of that group. For example, you decide about memberships within your group.

**To change or assign a group manager**

1. Open **Ownerships** and click **Claim ownership**
2. Perform one of the following tasks.
   a. Choose **Assign** to select a group.
   b. Choose **Change** to select a group.
3. Click **Claim ownership**.
   Your settings are saved.

**Auditing**

Auditing describes how an aspect of a company is assessed. Quality assurance is also plays an important part in auditing. An audit is a systematic, independent and documented examination, which assesses quality-related actions and evaluates them based on the planned requirements and targets. To successfully complete an audit there must be certain features available and specific requirements must be fulfilled.

If you are a manager or compliance officer, you have access to the **Auditing** menu. **Auditing** gives you read-only permission of any item for which you are responsible. You can use this to investigate any security issues that arise, or for similar activities. In many cases, you are able to manipulate the view to maximize its value, and export the information to a report.
Detailed information about this topic

- Employees on page 230
- System entitlements on page 234
- Business roles on page 227
- System roles on page 236
- Assignment resources on page 237
- Organizations on page 225
- Resources on page 233
- Assignment resources on page 237
- Multi-request resources on page 228
- Multi-requestable/unsubscribable resources on page 229
- Applications on page 226

Organizations

Departments, cost centers, locations, and business roles are each mapped to their own hierarchy under Organizations. This is due to their special significance for daily work schedules in many companies. Various company resources can be assigned to organizations, for example, authorizations in different SAP systems or applications. You can add employees to single roles as members. Employees obtain their company resources through these assignments when the One Identity Manager is appropriately configured.

Auditing of departments, cost centers and locations is always structured in the same way and is described here for all organizations on the basis of a department.

All departments are listed in Auditing, which you open from Department menu under Auditing. You can select an employee from here to view more details about their department.

After you have selected the department, you can gather more information through various views. You will know many of the views already from My Responsibilities.

Table 80: Overview of department views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the department in a Hyper View. This information might be assigned entitlements, for example.</td>
<td>To view all the information at one glance and navigate quickly to points of interest, click the linked content in the shapes. For creating reports.</td>
</tr>
<tr>
<td>Memberships</td>
<td>Show all employees that have access to the selected department</td>
<td>You can view the origin of an assignment for a selected employee. An</td>
</tr>
<tr>
<td>View</td>
<td>Description</td>
<td>Usage</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Master data</td>
<td>Shows the properties entered in the master data for the department.</td>
<td>View of properties entered. You can edit the manager, for example.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Shows all the assigned entitlements of the selected department.</td>
<td>To can view the analysis of the assignment in the detailed content view for the selected entitlement.</td>
</tr>
<tr>
<td>Risk</td>
<td>List properties and assignments, which contribute to the calculated risk index.</td>
<td>For viewing risk index functions.</td>
</tr>
<tr>
<td>Usage</td>
<td>Shows various role classes for viewing employee assignments for the selected department.</td>
<td>Select a role class to view employee assignments.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Lists all compliance rules for the selected department and their analysis.</td>
<td>For viewing compliance rule analyzes.</td>
</tr>
<tr>
<td>History</td>
<td>Displays the history of states and comparisons of the selected departments.</td>
<td>You can swap from timeline to table view. Navigate by clicking the mouse within the timeline.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Lists all attestation cases for the selected departments.</td>
<td>You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.</td>
</tr>
</tbody>
</table>

**Applications**

You can assign applications directly or indirectly to employees. Indirect assignment is carried out by assigning employees and applications to company structures, such as departments, cost centers, locations, or business roles. Assigned applications might be internet software, address management, mail, or text handling, for example.

All resources are displayed in a list in the **Auditing** view that you select through **Applications** in the **Auditing** menu. You can select an employee from here to view more details about their application.

After you have selected the application, you can gather more information through various views. You will know many of the views already from **My Responsibilities**.
Table 81: Overview of application views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the application in a Hyper View. This information</td>
<td>To view all the information at one glance and navigate quickly to</td>
</tr>
<tr>
<td></td>
<td>might be assigned service items, managers or system roles, for example.</td>
<td>points of interest, click the linked content in the shapes. For</td>
</tr>
<tr>
<td>Memberships</td>
<td>Show all employees that have access to the selected application.</td>
<td>creating reports.</td>
</tr>
<tr>
<td>Master data</td>
<td>Display the properties for the select application grouped under the master</td>
<td>View of properties entered. You can edit the service item, for</td>
</tr>
<tr>
<td></td>
<td>data.</td>
<td>example.</td>
</tr>
<tr>
<td>Usage</td>
<td>Shows various role classes for viewing employees who are members of the</td>
<td>Select a role class to view employee assignments.</td>
</tr>
<tr>
<td></td>
<td>selected service.</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>Lists all compliance rules and their analysis.</td>
<td>For viewing compliance rule analyzes.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Lists all attestation cases for the selected application.</td>
<td>You can selectively search for an attestation case and display</td>
</tr>
<tr>
<td></td>
<td></td>
<td>attestors for pending attestation cases or send reminders.</td>
</tr>
</tbody>
</table>

Business roles

All business roles are displayed in a list in Auditing that you select through Business Roles. You can select an employee from here to view more details about their roles and entitlements.

After you have selected the business role, you can gather more information through various views. You will know many of the views already from My Responsibilities.

Table 82: Overview of business role views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the business role in a hyper view. This information</td>
<td>To view all the information at one glance and navigate quickly to</td>
</tr>
<tr>
<td></td>
<td>might be assigned groups, for example.</td>
<td>points of interest, click the linked content in the shapes.</td>
</tr>
<tr>
<td>View</td>
<td>Description</td>
<td>Usage</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Memberships</td>
<td>Shows all employees that have access to the selected business role.</td>
<td>For creating reports.</td>
</tr>
<tr>
<td></td>
<td>You can view the origin of an assignment for a selected employee. An analysis of the assignment is shown in the detailed content view.</td>
<td></td>
</tr>
<tr>
<td>Master data</td>
<td>Shows the properties entered in the master data for the business role.</td>
<td>View of properties entered.</td>
</tr>
<tr>
<td></td>
<td>You edit the role class or the manager, for example.</td>
<td></td>
</tr>
<tr>
<td>Permissions</td>
<td>Shows all the assigned entitlements of the selected business role.</td>
<td>To can view the analysis of the assignment in the detailed content view for the selected entitlement.</td>
</tr>
<tr>
<td>Risk</td>
<td>List properties and assignments, which contribute to the calculated risk index.</td>
<td>For viewing risk index functions.</td>
</tr>
<tr>
<td>Usage</td>
<td>Shows various role classes for viewing employee assignments for the selected business role.</td>
<td>Select a role class to view employee assignments.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Lists all compliance rules for the selected business role and their analysis.</td>
<td>For viewing compliance rule analyzes.</td>
</tr>
<tr>
<td>History</td>
<td>Displays the history of states and comparisons of the selected business role.</td>
<td>You can swap from timeline to table view. Navigate by clicking the mouse within the timeline.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Lists all attestation cases of the selected business role.</td>
<td>You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.</td>
</tr>
</tbody>
</table>

**Multi-request resources**

Multi-request resources are resources that employees can request more than once in IT Shop. Requests are automatically canceled once approved. The resources are not explicitly assigned to employees. Examples include consumables such as pens or printing paper.

All resources are displayed in a list in Auditing that you select through Multi-request resources. You can select an employee from here to view more details about their resources.

After you have selected a resource, you can gather more information through various views. You will know many of the views already from My Responsibilities.
### Table 83: Overview of multi-request resource views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the multi-request resources in a Hyper View. This information might be assigned service items, for example.</td>
<td>To view all the information at one glance and navigate quickly to points of interest, click the linked content in the shapes. For creating reports.</td>
</tr>
<tr>
<td>Master data</td>
<td>Shows the properties entered in the master data for the resource.</td>
<td>View of properties entered. You can edit the service item, for example.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Lists all compliance rules and their analysis for the selected multi-request resource.</td>
<td>For viewing compliance rule analyzes.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Lists all attestation cases of the selected multi-request resource.</td>
<td>You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.</td>
</tr>
</tbody>
</table>

### Multi-requestable/unsubscribable resources

Multi-requestable/unsubscribable resources are resources that an employee can request more than once in the IT Shop but must be explicitly returned once they are no longer required. They are assigned to employees after approval has been granted and they remain assigned until the request is canceled.

All resources are displayed in a list in Auditing that you select through Multi-requestable/unsubscribable resources. You can select an employee from here to view more details about their resources.

After you have selected a resource, you can gather more information through various views. You will know many of the views already from My Responsibilities.

### Table 84: Overview of multi-requestable/unsubscribable resources views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the multi-requestable/unsubscribable resources in a Hyper View. This information might be assigned service items, for example.</td>
<td>To view all the information at one glance and navigate quickly to points of interest, click the linked content in the shapes. For creating reports.</td>
</tr>
<tr>
<td>Master data</td>
<td>Shows the properties entered in the master data for the resource.</td>
<td>View of properties entered. For example, you can edit the</td>
</tr>
</tbody>
</table>
### Compliance
Lists all compliance rules and their analysis for the selected multi-requestable/unsubscribable resource. For viewing compliance rule analyzes.

### Attestations
Lists all attestation cases of the selected multi-requestable/unsubscribable resources, You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.

### Employees
Any employees called from Employee under the Auditing menu are listed in the Auditing view. Here you can select an employee and view more details. You can select the employee directly from the list or use the Web Portal's filter function. For more information, see Filter on page 36.

After you have selected the employee directly from the list, you can gather more information through various views. You will know many of the views already from My Responsibilities.

#### Table 85: Overview of employee's views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Displays more details about the employee in a Hyper View. For example, active assignment requests.</td>
<td>To view all the information at one glance and navigate quickly to points of interest, click the linked content in the shapes. For creating reports.</td>
</tr>
<tr>
<td>Master data</td>
<td>Display the properties for the select employee grouped under the master data.</td>
<td>View of properties, for example, assigned role classes or the manager.</td>
</tr>
<tr>
<td>Requests</td>
<td>Lists all the selected employee’s requests.</td>
<td>Use the filter function and the advanced search to search selectively.</td>
</tr>
<tr>
<td>Rule violations</td>
<td>Lists all the selected employee’s rule violations.</td>
<td>Use the filter function and the advanced search to search selectively for rule violations.</td>
</tr>
<tr>
<td>Approvals</td>
<td>Lists all approvals in the selected period that the select</td>
<td>Use the filter function and the advanced search to search selectively</td>
</tr>
<tr>
<td>View</td>
<td>Description</td>
<td>Usage</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Risk</td>
<td>List properties and assignments, which contribute to the calculated risk index.</td>
<td>For viewing risk index functions.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Lists all the attestation cases of the selected employee.</td>
<td>You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Lists all compliance rules and their analysis for the selected employee.</td>
<td>For viewing compliance rule analyzes.</td>
</tr>
<tr>
<td>Roles and entitlements</td>
<td>Lists all the selected employee’s memberships.</td>
<td>Use the filter function to search selectively for memberships.</td>
</tr>
<tr>
<td>Ownerships</td>
<td>Shows ownerships of the selected objects type for this employee.</td>
<td>Shows a more detailed view of ownerships. Jump to more details on the highlighted role, entitlement or resource via Show details in the master detail.</td>
</tr>
<tr>
<td>History</td>
<td>Displays the history of states and comparisons of the selected employee.</td>
<td>You can swap from timeline to table view. Navigate by clicking the mouse within the timeline.</td>
</tr>
</tbody>
</table>

**Employee approvals**

Approvals in the Employee menu display any approvals in the selected time period for which the selected employee was involved. Approvals are spread over the following views.

- Approvals
- Exception approvals
- Attestations
- Policy violations

ℹ️ **NOTE:** The advanced search is only available in Approvals.
To search for an approval

1. Open Auditing | Employee and select an employee.
2. Ensure that Approvals is selected in the Approvals view.
3. Use the extended search.

Detailed information about this topic

- Searching on page 26
- Filter on page 36

Employee memberships

Roles and entitlements shows all an employee's memberships. This view is similar to Memberships under My Responsibilities.

To view employee memberships in more detail

1. Select Roles and entitlements.
2. Perform one of the following tasks:
   a. Use a filter and then mark the item you want in the result list.
   b. Mark the entry you want in the list.
      This displays details of the selected item in the detailed content view.

Detailed information about this topic

- Filter on page 36
- System entitlements on page 234
- Business roles on page 227

Application roles

One Identity Manager supplies default application roles whose permissions are matched to the different task and functions. Assign employees to default applications who take on individual tasks and functions. You can also create your own application roles for custom defined tasks.

NOTE: Default application roles are defined in One Identity Manager modules and are not available until the modules are installed. You cannot delete default application roles.
All application roles are displayed in a list in **Auditing**, which you open through One Identity Manager **Application Roles** in the **Auditing** menu. Here you can select an application role and view more details.

After you have selected a system role, you can use various views to obtain more information. You will know many of the views already from **My Responsibilities**.

### Table 86: Overview of application role views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the application role in a hyper view.</td>
<td>To view all the information at one glance and navigate quickly to points of interest, click the linked content in the shapes. For creating reports.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Lists all compliance rules for the selected application role and their analysis.</td>
<td>For viewing compliance rule analyzes.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Lists all attestation cases for the selected application role.</td>
<td>You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.</td>
</tr>
</tbody>
</table>

### Resources

Resources are found in One Identity Manager in IT resources and non-IT resources. Non-IT resources help an employee's work efficiency, for example, mobile phones, desks, company cars, or keys. You can assign resources directly to an employee or through classification into hierarchical roles. Similarly, you can resources request for an employee through the IT Shop. Resources are divided up from a functional point of view.

- Resources
- Multi-request resources
- Multi-requestable/unsubscribable resources

An employee can own resources (workstation, device) just once. They can be requested exactly once in the IT Shop. The resources are assigned to the employees after approval has been granted. They remain assigned until the request is canceled. You can request them again a later point. Examples are telephones or company cars.

All resources are displayed in a list in **Auditing** that you select through **Resources** in the **Auditing** menu. You can select an employee from here to view more details about their resources.

After you have selected a resource, you can gather more information through various views. You will know many of the views already from **My Responsibilities**.
Table 87: Overview of resource views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the resource in a Hyper View. This information might be assigned service items or employees, for example.</td>
<td>To view all the information at one glance and navigate quickly to points of interest, click the linked content in the shapes. For creating reports.</td>
</tr>
<tr>
<td>Memberships</td>
<td>Shows all employees that have access to the selected resource.</td>
<td>You can view the origin of an assignment for a selected employee. An analysis of the assignment is shown in the detailed content view.</td>
</tr>
<tr>
<td>Master data</td>
<td>Shows the properties entered in the master data for the department.</td>
<td>View of properties entered. You can edit the service item, for example.</td>
</tr>
<tr>
<td>Usage</td>
<td>Shows various role classes for viewing employees who are members of the selected service.</td>
<td>Select a role class to view employee assignments.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Lists all compliance rules for the selected resource and their analysis.</td>
<td>For viewing compliance rule analyzes.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Lists all attestation cases for the selected resources.</td>
<td>You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.</td>
</tr>
</tbody>
</table>

**System entitlements**

In **Auditing**, you can view the entitlements assigned to an employee for the particular target system type that they manage. Each target system type has its own tile in the **Auditing** view.

Auditing of system entitlements is the same for all target system types and is therefore described here for all of them together.

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. The following system entitlements are displayed in the **Auditing** menu, for example.

- Active Directory groups
- SAP groups
- SharePoint groups
After you have selected the system entitlement, you can gather more information through various views. You will know many of the views already from My Responsibilities.

### Table 88: Overview of system entitlement views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the system entitlement in a HyperView. This might be the target system that is assigned, user accounts and service item, for example.</td>
<td>To view all the information at one glance and navigate quickly to points of interest, click the linked content in the shapes. For creating reports.</td>
</tr>
<tr>
<td>Memberships</td>
<td>Shows all employees that have access to the selected system entitlement.</td>
<td>You can view the origin of an assignment for a selected employee. An analysis of the assignment is shown in the detailed content view.</td>
</tr>
<tr>
<td>Master data</td>
<td>Shows the properties entered in the master data for the system entitlement.</td>
<td>View of properties entered. You can, for example, edit service items or set the risk index.</td>
</tr>
<tr>
<td>Child groups</td>
<td>Shows assigned sub groups.</td>
<td>Here you can see which groups are members in the selected system entitlement.</td>
</tr>
<tr>
<td>Usage</td>
<td>Show various role classes for viewing employee assignments for the selected system entitlement.</td>
<td>Select a role class to view employee assignments.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Lists all compliance rules for the selected system entitlement and their analysis.</td>
<td>For viewing compliance rule analyzes.</td>
</tr>
<tr>
<td>History</td>
<td>Displays the history of states and comparisons of the selected system entitlement.</td>
<td>You can swap from timeline to table view. Navigate by clicking the mouse within the timeline.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Lists all attestation cases for the selected system entitlement.</td>
<td>You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.</td>
</tr>
</tbody>
</table>

### Viewing an employee's system entitlements

The view for an employee's system entitlements are explained on the basis of an Active Directory group example.
**To view an Active Directory group's system entitlements**

1. Select the target system in the **Auditing** Active Directory menu.
2. Select an employee in **Auditing - Active Directory** using **Change**.
   This displays the system entitlements assigned to the employee.
3. Click **Show details**.
   This displays other view for the selected system entitlement.

**System roles**

All system roles are displayed in a list **Auditing** view that you select through **System Roles** in **Auditing**. You can select an employee from here to view more details about their roles and entitlements.

After you have selected a system role, you can use various views to obtain more information. You will know many of the views already from **My Responsibilities**.

**Table 89: Overview of system role views**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the system role in a Hyper View. This information might be the groups that are assigned, service item or employees, for example.</td>
<td>To view all the information at one glance and navigate quickly to points of interest, click the linked content in the shapes. For creating reports.</td>
</tr>
<tr>
<td>Memberships</td>
<td>Shows all employees that have access to the selected system role.</td>
<td>You can view the origin of an assignment for a selected employee. An analysis of the assignment is shown in the detailed content view.</td>
</tr>
<tr>
<td>Master data</td>
<td>Shows the properties entered in the master data for the system role.</td>
<td>View of properties entered. You can, for example, edit service items or system role's supervisor.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Shows all the assigned entitlements of the selected system role.</td>
<td>To can view the analysis of the assignment in the detailed content view for the selected entitlement.</td>
</tr>
<tr>
<td>Risk</td>
<td>List properties and assignments that contribute to the calculated risk index.</td>
<td>For viewing risk index functions.</td>
</tr>
<tr>
<td>Usage</td>
<td>Shows various role classes for viewing employee assignments for the selected system</td>
<td>Select a role class to view employee assignments.</td>
</tr>
</tbody>
</table>
### View | Description | Usage
---|---|---
Compliance | Lists all compliance rules for the selected system role and their analysis. | For viewing compliance rule analyzes.
History | Displays the history of states and comparisons of the selected system role. | You can swap from timeline to table view. Navigate by clicking the mouse within the timeline.
Attestations | Lists all attestation cases of the selected system role. | You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.

### Assignment resources

Use assignment resources to request hierarchical roles, such as departments or business roles and assign them to employees, devices and workdesks. This means, for example, you can limit assignment resources to a certain business roles, which makes it unnecessary to select the business role additionally when you request an assignment resource. It is automatically a part of the assignment request. Assignment resources are available for requesting in the shop "Identity & Access Lifecycle". For more information about assignment resources, see the One Identity Manager Business Roles Administration Guide and One Identity Manager IT Shop Administration Guide.

**To display assignment resources**

1. In the menu bar, click Responsibilities | Auditing.
2. On the Auditing page, click the Assignment resources tile.

On the Auditing - assignment resources, all resources are displayed in a list. You can select an employee from here to view more details about their resources.

After you have selected an assignment resource, you can gather more information through various views. You will know many of the views already from My Responsibilities.

**Table 90: Overview of assignment resources**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Shows more details about the resource in a Hyper View. This information might be assigned service items, for example.</td>
<td>To view all the information at one glance and navigate quickly to points of interest, click the linked content in the shapes. For creating reports.</td>
</tr>
</tbody>
</table>
### View

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master data</td>
<td>Shows the properties entered in the master data for the assignment resource.</td>
<td>View of properties entered. For example, you can edit the resource type or the service item.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Lists all compliance rules for the selected assignment resource and their analysis.</td>
<td>For viewing compliance rule analyzes.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Lists all attestation cases for the selected assignment resource.</td>
<td>You can selectively search for an attestation case and display attestors for pending attestation cases or send reminders.</td>
</tr>
</tbody>
</table>

### Governance administration

In Governance Administration, which you reach through Responsibilities, you can edit business roles or system entitlements as a target system administrator. You can make the following changes, for example:

- Add a new owner role to an Active Directory group and assign a new product owner.
- Edit an Active Directory group's requestability.
- Modify entitlement properties.

#### Detailed information about this topic

- [Business roles](#) on page 238
- [System entitlements](#) on page 240
- [Organization](#) on page 242

### Business roles

As a business role administrator, you can view every role in the Governance Administration menu and edit them. Deleted roles can be restored.

#### To view business roles

1. Open Responsibilities | Governance Administration and click Business Roles.
   
   By default, all roles are listed with their names, managers and roles classes. Use Additional columns to display more detailed about the business classes.

2. Marked the required role.
To search for the role you want, you have the usual help available such as a filter function, filter wizard, and the search function. For more information, see Navigation and use on page 18.

**Detailed information about this topic**

- Editing business roles on page 239
- Restoring deleted roles on page 240

**Editing business roles**

In **Governance Administration**, edit properties on all business roles as an administrator.

In **My responsibilities**, edit the business roles that you manage. You will find this content listed under "Detailed information about this topic" because the method of editing is the same for both menus, and each editing step in **My Responsibilities** has already been described.

**To edit a role**

- Select the required role and click **Edit** in the master detail.
  
  This open a view for the selected role with more selection options, which you will recognize from **My Responsibilities**.

**Detailed information about this topic**

- Master data on page 168
- Adding memberships on page 159
- Deleting memberships on page 160
- Adding entitlements on page 169
- Deleting entitlements on page 170
- Splitting a role on page 170
- Viewing risk indexes on page 149
- Splitting a role on page 170
- Compare and merge on page 174
- History on page 152
- Timeline on page 153
- Status comparison on page 154
- Restoring a previous state on page 175
- Usage on page 163
- Compliance reports on page 176
- Attestations on page 177
Restoring deleted roles

Another function for managing roles is restoring deleted roles. An example of a deleted role could be roles that have been sorted out during merging.

This function is also available in the views of managed organizations. Restoring a deleted role is described in the following step-by-step on the basis of a business role.

To restore deleted roles

1. Perform one of the following tasks.
   - Open the Business roles menu and Restore a deleted role.
   - OR -
   - Restore a lower-level role by selecting a business role in the Business roles menu and clicking Restore.

This opens a dialog. The view Select deleted role is enabled and lists all the deleted objects.

   NOTE: You can set a date in order to limit your search for deleted roles.

2. Select the desired role and click Next.

Multi-select is possible. The view Verify appears and lists the actions that will be run on restore.

3. You can deselect individual actions if you do not want to run them all. Click Continue.

4. Close the dialog.

System entitlements

You will find the target system manager responsibilities under Governance Administration.

- Add a new owner role and assign a product owner to an Active Directory group if you are target system administrator. You can also edit the requestability of an Active Directory group.

- Change the properties of the entitlement. For more information, see Master data on page 168.

To open the "System Entitlements" menu

- Open Responsibilities | Governance Administration and click System Entitlements.
Detailed information about this topic

- Assigning product owners on page 241
- Assigning attestors on page 241

Assigning product owners

In the Governance Administration menu, you can assign a new product owner to an Active Directory group.

To assign a new product owner

1. Open System entitlements and select the required Active Directory group.

   NOTE: This function is only available if the module Active Directory Module is installed.

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

2. Select the Owner view and click New.

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

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

4. Select a product owner using Assign and the new owner role via Product owner.

   NOTE: If Without owner in AD was selected in Product owner, you cannot select a product owner.

Assigning attestors

In the Governance Administration menu, you can assign an attestor to an Active Directory group.

To assign an attestator

1. Open System entitlements and select the required Active Directory group.

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

2. Select the Attestor view and click New.

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

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

4. Use Assign to select attestors and select the new application role via Attestors.
Organization

As administrator, you can view and edit all the organizations in Governance Administration. Deleted roles can be restored. Organizations are divided into cost centers, departments, and locations.

To select an organization

1. Open Responsibilities | Governance Administration and click Organization. This opens Organization.
2. Select the organization type required. This lists all the roles belonging to the selected organization type. Use Additional columns to display more details about the organization type.
3. Marked the required role. To search for the role you want, you have the usual help available such as a filter function, filter wizard, and the search function. For more information, see Navigation and use on page 18.

Detailed information about this topic

- Editing roles on page 242
- Restoring roles on page 243

Editing roles

You can edit roles in Governance Administration under Organizations.

To edit a role

1. Select the required role and click Edit in the master detail. This open a view for the selected role with more selection options, which you will recognize from My Responsibilities.
2. Perform one of the following tasks:
   a. Edit the master data.
   b. Request or delete memberships.

Detailed information about this topic

- Master data on page 168
- Adding memberships on page 159
- Deleting memberships on page 160
Restoring roles

In Governance Administration under Organizations, you can restore deleted roles.

To restore a deleted role

1. Select the required role and click Restore a deleted role in the master detail. This opens a dialog. The view Select deleted role is enabled and lists all the deleted objects.

   **NOTE:** You can also select Select a deleted role before you select the organization type.

   **NOTE:** You can set a date in order to limit your search for deleted roles.

2. Select the desired role and click Next.

   Multi-select is possible. The view Verify appears and lists the actions that will be run on restore.

3. You can deselect individual actions if you do not want to run them all. Click Continue.

4. Close the dialog.
Applications

You may be able to access other applications, as configured by your system administrator. This provides you with a shortcut to other web applications deemed of value by your company.

**NOTE:** If you are a system administrator, and would like to add applications, see the One Identity Manager Web Designer Reference Guide.

**To access other web applications from the Web Portal**

- Open **Applications** and select the required web application.
  
  The application may appear within the Web Portal, or in a separate window, depending on how the system administrator configured it.
Calls

In the **Calls** menu, you can add new calls or view all calls in the call history.

**Detailed information about this topic**

- Adding new calls on page 245
- Call history on page 245

**Adding new calls**

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

**To add a new call**

1. Open **New Call**.
2. Enter a detailed description of the problem and select the affected product.
3. Set the severity of the problem in **Severity** and select a cost center using **Assign**.
4. Select an additional employee via **Assign** and click **Save**.

**Call history**

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

ℹ️ **NOTE:** Use the check boxes at the top of the section to limit the calls shown.
To view a specific call

1. Open Call history and select a call from the list.
   More information about the call is displayed in the detailed content view. You can subsequently change Severity, Description and Product entries on the Master Data tab.
2. View the staff involved, status and measures taken on the History tab.
3. View attachments on the Attachments tab.
4. Click Save.

Removing attachments

In the Call History menu, you can remove single files that have been added as attachments to a call.

To delete a file from a call's attachments

1. Open Call history and select a call from the list.
2. Select Attachments in the master detail and click next to the file.
3. Confirm the message with Yes.
   This deletes the file from the attachments.
TheSettingsmenu is below the header on the right-hand side of the screen. When you open this option, My Settings view is displayed with more possible options.

Detailed information about this topic
- Mail subscriptions on page 247
- Personal dashboard settings on page 248
- Subscriptions on page 248
- Reports on page 252

Mail subscriptions

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

- Attestation - reject approval
- Attestation - answer
- Attestation - approval required
- Attestation - delegated/additional approval
- Attestation - remind approver
- Attestation - question
- Report subscription - delivery
- Report subscription - delivery to cc
- IT Shop request - canceled
- IT Shop request - aborted
- IT Shop request - expired
- IT Shop request - reject approval
- IT Shop request - answer
- IT Shop request - approval required
- IT Shop request - delegated/additional approval
- IT Shop request - remind approver
- IT Shop request - escalation
- IT Shop request - question
- IT Shop request - not granted approval
- IT Shop request - approval not granted to approval step
- IT Shop request - granted approval
- IT Shop request - approval granted to approval step
- IT Shop request - product expires
- IT Shop request - product change

To subscribe or unsubscribe mail

1. Open the Settings menu and click Mail Subscriptions.
2. Enable the checkbox Receive email on the required mail template and click Save.

Personal dashboard settings

In Personal Dashboard Settings, you can hide or show dashboards with neutral trends. Dashboards with "neutral trends" are those that have not change recently. By default, this filter is not enabled. You can also hide other dashboards. To hide individual dashboard, you can use the filter function on the desired dashboard view. For more information, see Hiding statistics on page 260.

To show a dashboard

1. Open Personal Dashboard Settings.
2. Perform one of the following tasks.
   a. Enable Show dashboards with neutral trends.
   b. Select one of the displayed statistics that you want to display again.
3. Click Save.

Subscriptions

Subscriptions can be found in Web Portal under Settings.
The reports you have subscribed are listed in **Subscriptions**. You can modify your report subscriptions or subscribe to new reports. In the following table, actions are listed that you can run on subscribed reports.

**Table 91: Actions for subscribed reports**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📝</td>
<td>Edit subscription settings.</td>
</tr>
<tr>
<td>📲</td>
<td>Add employees to this subscription.</td>
</tr>
<tr>
<td>📩</td>
<td>Send report now.</td>
</tr>
<tr>
<td>✖</td>
<td>Cancel the subscription.</td>
</tr>
</tbody>
</table>

**Detailed information about this topic**

- Adding subscriptions on page 249
- Editing subscription settings on page 250
- Receive subscription immediately on page 251
- Ending subscriptions on page 251

**Adding subscriptions**

In **My Subscriptions**, you can add new subscriptions.

**To add a subscription**

1. Open **My Subscriptions** and click **Add subscription**.
2. Mark the report you want to subscribe to in **Available reports** and click **Next**.
3. Set the following options in **Edit report parameters** and save the changes.

**Table 92: Editing subscription settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription</td>
<td>Field for entering or editing the subscription name.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Menu for selecting how often the report is sent. The following options are available:</td>
</tr>
<tr>
<td></td>
<td>- Monthly report subscriptions</td>
</tr>
<tr>
<td></td>
<td>- half-yearly report subscriptions</td>
</tr>
<tr>
<td></td>
<td>- Yearly report subscriptions</td>
</tr>
<tr>
<td></td>
<td>- Quarterly report subscriptions</td>
</tr>
</tbody>
</table>
### Editing subscription settings

In **My Subscriptions**, you can edit your subscriptions at any time.

**To edit subscription settings**

1. Open **My Subscriptions** and select a subscribed report.
   
   More information about this report is displayed in the detailed content view; for example, how often it appears or any additional subscribers.

2. Click 📝 in the detailed content view.

3. Edit the following settings in **Edit subscription settings** and save the changes.

**Table 93: Editing subscription settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription</td>
<td>Field for entering or editing the subscription name.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Menu for selecting how often the report is sent. The following options are available:</td>
</tr>
<tr>
<td></td>
<td>• Monthly report subscriptions</td>
</tr>
<tr>
<td></td>
<td>• half-yearly report subscriptions</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Yearly report subscriptions</td>
</tr>
<tr>
<td></td>
<td>• Quarterly report subscriptions</td>
</tr>
<tr>
<td></td>
<td>• Daily report subscriptions</td>
</tr>
<tr>
<td></td>
<td>• Weekly report subscriptions</td>
</tr>
</tbody>
</table>

**Format (e-mail attachment)** | **Menu for selecting the report format. The report can be sent in the following formats:**
- CSV
- DOCX
- HTML
- PDF
- RTF
- TEXT
- TIFF
- XLS
- XLSX
- XML
- XPS

**Receive subscription immediately**

You can receive you subscribed report immediately in **My Subscriptions**.

**To receive a subscription immediately**

1. Open **My Subscriptions** and select a subscribed report.
2. Click ✉️ in the detailed content view.

   A message is displayed in **My Subscriptions** to inform you that an email has been sent with the report to your email address.

**Ending subscriptions**

You can end report subscription in **My Subscriptions**.
To end a subscription

1. Highlight the required report in My subscriptions and click in the master detail.
2. Confirm with Yes.

Reports

You will find report in the Web Portal under the Settings.
You can view and edit reports in the Reports view. You can also create your own reports and organizations or assign employee.

Detailed information about this topic

- New report on page 252
- Viewing report definitions on page 253
- Displaying reports on page 256
- Exporting reports on page 256

New report

You can add new reports in the Reports view. To do this, you enter the master data.

MOBILE: This function is not available in the mobile interface.

To create a report

1. Click New report in Reports.
2. Configure the following in the Create a new report view.

NOTE: Any fields that are not marked with an asterisk (*) are optional. Optional fields can be filled in when you create the application or at a later stage.

Table 94: Master data for a new report

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name*</td>
<td>Field for the report name. Enter the report’s name.</td>
</tr>
<tr>
<td>Report definition</td>
<td>Select the base table with Assign. You can edit the selected base table using Result</td>
</tr>
</tbody>
</table>
Once a base table has been assigned, you can change the assignment with **Change**.

Risk index
Display a scale of 0 to 1 for the risk index and two slide rulers.
Specify a beginning and an end value within the scale.

Owner
Name of the report owner.
Use **Change** to select from a list of owners.

Service item
Creating a new service item.
Use **Create a new service item** to create a new product.
You can disable this report definition using **Disable**.

Assign to employees
Selecting other employees as report recipients.
Use **Change** to select an employee to receive the report.

Assign to departments
Selection of departments to receive the report.
Use **Assign** to select a department to receive the report.

Assign to Locations
Selection of locations to receive the report.
Use **Assign** to select a location to receive the report.

Assign to cost centers
Selection of cost centers to receive the report.
Use **Assign** to select a cost center to receive the report.

3. Click **Save**.

**Viewing report definitions**

Use **View report definition** to view more information about an existing report and make changes if required.

- Overview
  View assigned properties of the selected report in a Hyper View.
- Master data
Edit and modify report properties.

- **Usage**
  View employee assignments to a role class.

**Detailed information about this topic**

- [Overview](#) on page 254
- [Master data](#) on page 254
- [Usage](#) on page 256

**Overview**

With **View report definition**, you open, among other things, an overview of the selected report. All relevant information about the report is provided in abbreviated form in the overview, such as, assigned employees or application roles. They are displayed in shape elements.

**To view an report's overview**

1. Open **Reports** and select the report you want to view.
2. Click **View report definition**.
3. Select **Overview** to view all the information about an employee at a glance.

**Master data**

Use **View report definition** to open the master data to add missing properties or to edit properties such as the risk index.

**To edit the master data**

1. Open the menu **Settings** and click **Reports**.
2. Select a report and click **View report definition**.
3. Select **Master data** and edit the following settings.

**NOTE:** Any fields that are not marked with an asterisk (*) are optional. Optional fields can be filled in when you create the application or at a later stage.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name*</td>
<td>Field for the report name. Enter the report’s name.</td>
</tr>
<tr>
<td>Report definition</td>
<td>Base table selection. Use <strong>Change</strong> to select the base table you want from a list.</td>
</tr>
<tr>
<td>Risk index</td>
<td>Display a scale of 0 to 1 for the risk index and two slide rulers. Specify a beginning and an end value within the scale.</td>
</tr>
<tr>
<td>Owner</td>
<td>Name of the report owner. Use <strong>Change</strong> to select from a list of owners.</td>
</tr>
<tr>
<td>Service item</td>
<td>Creating a new service item. Use <strong>Create a new service item</strong> to create a new product. You can disable this report definition using <strong>Disable</strong>.</td>
</tr>
<tr>
<td>Assign to employees</td>
<td>Selecting other employees as report recipients. Use <strong>Change</strong> to select an employee to receive the report.</td>
</tr>
<tr>
<td>Assign to departments</td>
<td>Selection of departments to receive the report. Use <strong>Assign</strong> to select a department to receive the report.</td>
</tr>
<tr>
<td>Assign to Locations</td>
<td>Selection of locations to receive the report. Use <strong>Assign</strong> to select a location to receive the report.</td>
</tr>
<tr>
<td>Assign to cost centers</td>
<td>Selection of cost centers to receive the report. Use <strong>Assign</strong> to select a cost center to receive the report.</td>
</tr>
</tbody>
</table>

4. Click **Save**.
Usage

Through View report definition, you can view employee assignments to a role class on Usage.

To view which roles are contained in a predefined report

1. Mark a report in Reports view and click View report definition.
2. Select the Usage view.
3. Select a role class in the Role classes menu to see the roles contained in the report.
4. Select More information to view employees assigned to the role memberships.

Displaying reports

You can display a report completely in the Reports view. For example, all departments with managers and calculated risk index, are displayed for the report "Departments with increased violations".

To view the base table configured for the report

- Mark a report in the Reports view and click View report in the detailed content view.
  - The base tables for this report are shown in the report view.

Exporting reports

Reports can help you to make necessary decisions. For example, when you are viewing your file system or SharePoint resources, you can view reports to help determine ownership. Or when you are performing attestations, you can view current information on the item to which you are attesting.

1. Select Export this view.
   - This opens the Export this view dialog. You have several options.
2. Enable the following setting if necessary.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All pages</td>
<td>All pages of the view were exported. If this setting is not enabled, only the current page is exported.</td>
</tr>
<tr>
<td>Remove header</td>
<td>This setting is only available for CSV format.</td>
</tr>
</tbody>
</table>
3. Perform one of the following tasks:
a. Select either **Export as PDF**.
b. Select the option **Export as CSV**.
c. Select **Show as web page**.

The report is exported in the respective format.
Discovering your statistics on the start page

Statistics are graphical summaries of the information pertaining to you. You can open your statistics on the start page taking your access permissions and entitlements into account.

**NOTE:** In earlier versions of the Web Portal, these statistics are located under Access Governance.

More statistics about managed organizations, system entitlements, business roles and system roles are available for managers in My Responsibilities.

The data on the start page is updated daily. You can customize the data you see on the dashboard by selecting the objects you want to include, and which statistics you want to show for each object. Checking your dashboard regularly can help you understand any issues that need addressing. For more information, see What statistics are available? on page 263.

**Detailed information about this topic**

- Statistics on page 258
- Heatmap on page 261
- What statistics are available? on page 263

**Statistics**

Graphical representation of data is depicted by diagrams. Heatmaps also provide data in graphical form. For more information, see Heatmap on page 261.

**Table 96: Icons used in diagrams**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>The value in this statistic is in the balance. It is neither critical nor compliant. You should keep an eye on this value or statistic.</td>
</tr>
</tbody>
</table>
### Icon | Meaning
--- | ---
> This value has not changed. The date of last change is shown.

This icon verifies that the value in this statistic compliant. The arrow icon displayed in combination with this icon is also green and provides more detailed information about changes to the value.

This icon indicates that the value in this statistic is in the critical range. The arrow icon displayed in combination with this icon also means critical and provides more detailed information about changes to the value.

This arrow icon shows an increasing value since the last change and is colored green. The value is still in a compliant range. The difference since the last change is shown.

This arrow icon shows a decreasing value since the last change and is colored green. The value is still in a compliant range. Moving the mouse over the icon shows the change since the last change.

This arrow icon shows an increasing value since the last change and is colored red. The value is in the non-compliant range and more critical than before. The difference since the last change is shown.

This arrow icon shows a decreasing value since the last change and is colored red. The value is in the non-compliant range but better than before. Moving the mouse over the icon shows the difference since the last change.

### Detailed information about this topic
- Viewing statistics on page 259
- Hiding statistics on page 260
- Viewing source data on page 260
- Apply filter on page 260

### Viewing statistics

The use of Hyper Views, heatmaps and statistics differs between the desktop view and the mobile view. For more information, see Heatmaps and statistics in the mobile view on page 48.

**To open a statistics view**

1. Select the start page 🏡.
   - Roles and organizations are displayed on the start page.
2. Click the role or organization you want to see in more detail.
Depending on your selection, you are shown statistics either in form of a table or a heatmap. There are also, however, roles or organizations, which take you to a page with source data.

**Hiding statistics**

You can hide statistic, which are not relevant. These you can show again at any time over your **Personal Dashboard Settings** in the **Settings**. For more information, see **Personal dashboard settings** on page 248.

**To hide statistics**

1. Select the start page via 🏡.
   Roles and organizations are displayed on the start page.
2. Click the role or organization you want to see in more detail.
3. Click ⬇️ the selected role’s view.
4. Disable one or more statistics in the list that you do not want to see anymore.
5. Close the dialog.
   This hides the selected statistics.

**Viewing source data**

You can only view source data for certain roles and organizations. You can view a heatmap or statistics, with graphical representation, through certain roles or organizations.

**To view source data from a role or organization**

1. Select the start page.
   Roles and organizations are displayed on the start page. These roles or organizations are divided into their associated subgroups.
2. Click the role or organization you want to view in more detail, for example, departments without managers.
   This displays a view with the corresponding data.

**Apply filter**

You can filter the information displayed on your dashboard to suit your own requirements.
To customize the information displayed on a statistics view

- Apply a filter to the statistic view.
  This opens a dialog for the selected filter. For more information, see Filter on page 36.

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

Heatmap

The heatmap in the Web Portal presents roles and organizations as colored squares. They are intended to help you quickly visualize particularly prominent values within a large amount of data and to comprehend them at a glance. The size of the rectangles corresponds to the relative size of the role or organization. The more employees you have in a company’s structure, for example, the larger the rectangle in the view.

  NOTE: An overview of the company structures you manage is displayed on the start page.

The rectangle colors correspond to a selectable, linked-in data value, and range from red to green, where red stands for a value tending to require more attention. Red indicates, for example, a lot of compliance rule violations or employees with high risk indexes. Yellow indicates for an average, which can also mean that there has been no changes to this company structure since the last analysis. The heatmap not only provides a clear overview of the current data, but also provides another useful function by making a historical comparison to previous data.

You can see the following risky results or properties in a heatmap.

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

  NOTE: Hyper Views, heatmaps and statistics have different behavior in the desktop view as opposed to the mobile view. For more information, see Heatmaps and statistics in the mobile view on page 48.

Detailed information about this topic

- Viewing data on page 262
- Viewing changes for a specific period on page 262
Limiting the amount of data on page 262
Displaying object details on page 263

Viewing data

Without having set any preferences, the color map is displayed as a data value when you open it, for example, for the number of compliance rules.

To view data from a role or organization

1. Select the start page.
2. If available, click the role or organization in the form of a heatmap that you would like to view more closely.
   - **NOTE:** In the first field, you can set the size of the square. Available settings are Dynamic size and Unisize.
3. Limit your selection by selecting one or more objects with Change.
4. Confirm your selection by clicking Close.
   - You selection is displayed to the left of Change.

Viewing changes for a specific period

In a heatmap you can view data within a specific time period.

To view data for a specific time period

- Select the required entry from the second field, for example "Month-to-date changes".
  - The data is displayed in the heatmap according to your selection.

Limiting the amount of data

You can limit the amount of data displayed in the heatmap by using the slide rule.

To limit the size of the data

- Click one of the slide rules in the scale at the bottom of the view to limit the data size.
  - **NOTE:** You may be shown up to 500 data sets graphically.
Displaying object details

To get more information, you can call up object details about an rectangle in a heatmap.

To obtain more information about individual roles or organizations

1. Click the rectangle in the view after you have configured your settings and the Web Portal has adjusted the view accordingly.

Another shape is displayed for the rectangle with additional information.

NOTE: To display additional information about the role or organization you are interested in, hover the mouse over the corresponding rectangle. This information is not so comprehensive and is there to provide initial orientation within the heatmap.

2. Perform one of the following tasks:
   a. Click one of the items to obtain more information.
   b. Select more information through View object details.

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

What statistics are available?

The statistics and heatmaps you see in Web Portal depend on your roles and permissions. Only statistics relevant to you are available on the start page.

Statistics can be customized to display the objects and statistics that interest you. You can also sort and filter statistical information or export it as a report. For more information, see Discovering your statistics on the start page on page 258.

Detailed information about this topic

- High-risk overview on page 264
- Compliance on page 264
- Risk on page 265
- Policies on page 266
- Organization on page 266
- IT shop on page 267
- Attestations on page 268
- Target systems on page 268
High-risk overview

This overview lists high-risk objects and divides them into different groups that can be expanded and collapsed. Each of the groups displays resources with the highest risk factor, which you manage. Risk indexes are calculated for employees, user accounts, system roles, structures, organizations, and business roles. Risk indexes are calculated for employees, user accounts, system roles, IT Shop structures, organizations and business roles, file systems, and SharePoint resources. Object have risk values, which provide the risk index when combined with risk index functions. You can view the following information in High-Risk Overview.

- Breakdown for of the highest-risk items for each type
- For more information on risk function calculators, see Modifying Risk Calculators.

Compliance

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

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

Statistics are available on the following topics.

Table 97: Overview of statistics on compliance rules

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending rule violations</td>
<td>Show all types of rule violations.</td>
</tr>
<tr>
<td>Compliance violations</td>
<td>Shows compliance violations</td>
</tr>
<tr>
<td></td>
<td>This statistic is available for different company structures.</td>
</tr>
<tr>
<td></td>
<td>• Department</td>
</tr>
<tr>
<td></td>
<td>• Location</td>
</tr>
<tr>
<td></td>
<td>• Cost center</td>
</tr>
<tr>
<td></td>
<td>• Business role</td>
</tr>
<tr>
<td>Compliance violations according to rules</td>
<td>Shows compliance rule violations for each rule.</td>
</tr>
<tr>
<td>New rule violations</td>
<td>Show new rule violations.</td>
</tr>
<tr>
<td></td>
<td>This statistic is also available for new rule violations in recent months.</td>
</tr>
</tbody>
</table>
### Statistics

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overdue rule violations</td>
<td>Shows overdue rule violations.</td>
</tr>
<tr>
<td>Assignments that contribute to violations</td>
<td>Show assignments that contributed to violations.</td>
</tr>
<tr>
<td>Last approvals granted (rule violations)</td>
<td>Show the last granted approvals that contributed to rule violations.</td>
</tr>
</tbody>
</table>
| Cost centers with increased violations       | Show the cost centers that stand out due to a high rate of violations.  
This statistic is also available for other company structures.  
  - Departments  
  - Locations |
| Last approvals (rule violations)             | Show the last approvals that contributed to rule violations. |

For more information, see [Governance administration](#) on page 133.

### Risk

There are various statistics available to you for risk assessment. The following statistics are available for this topic.

#### Table 98: Risk assessment statistics

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of active employees with a risk index of more than 0.5</td>
<td>Shows the number of active employees with a risk index more than critical value.</td>
</tr>
</tbody>
</table>
| Highest person risk index by department      | Show the highest risk index of all employees by department.  
This statistic is also available for other company structures.  
  - Location  
  - Cost center  
  - Business role |
| Average person risk index by department      | Shows the average risk index of employees by department.  
This statistic is also available for other company structures.  
  - Location |
### Statistics

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost center</td>
<td></td>
</tr>
<tr>
<td>Business role</td>
<td></td>
</tr>
<tr>
<td>Employees by risk index</td>
<td>Show all employees in groups of risk index in the same range.</td>
</tr>
</tbody>
</table>

### Policies

Other, different statistics are available for company policies.

**Table 99: Company policy statistics**

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending Policy Violations</td>
<td>Shows pending policy violations.</td>
</tr>
<tr>
<td>Overdue policy violations</td>
<td>Shows overdue policy violations.</td>
</tr>
<tr>
<td>Policy violations by department</td>
<td>Shows policy violations by department.</td>
</tr>
<tr>
<td></td>
<td>This statistic is available for different company structures.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Cost center</td>
<td></td>
</tr>
<tr>
<td>Business role</td>
<td></td>
</tr>
<tr>
<td>New policy violations</td>
<td>Shows new policy violations.</td>
</tr>
<tr>
<td></td>
<td>This statistic is also available for new policy violations within the last month.</td>
</tr>
<tr>
<td>Policy violations (actual)</td>
<td>Shows current policy violations.</td>
</tr>
<tr>
<td></td>
<td>This statistic is also available for new policy violations within the last seven days.</td>
</tr>
<tr>
<td>Policy violation approval rates</td>
<td>Shows the approval rate for policy violations.</td>
</tr>
<tr>
<td>Last approvals (policy violations)</td>
<td>Show the last approvals, which contributed to policy violations.</td>
</tr>
<tr>
<td>Last approvals granted (policy violations)</td>
<td>Show the last granted approvals, which contributed to policy violations.</td>
</tr>
</tbody>
</table>

### Organization

The following statistics are displayed for departments you manage.
- Information about employee accounts
- Information about employees
- Rule violations
- Information about pending requests
- The top roles and entitlements

For more information, see Departments on page 181.

**IT shop**

The shop is the mechanism employees use to make requests. These statistics help you to answer the following questions.

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

**Table 100: Statistics about IT shop structures**

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending requests</td>
<td>Displays all pending requests.</td>
</tr>
<tr>
<td>Open requests by service category</td>
<td>Displays all pending requests by service category. This statistic contains other criteria.</td>
</tr>
<tr>
<td></td>
<td>- By next approver</td>
</tr>
<tr>
<td></td>
<td>- By recipient</td>
</tr>
<tr>
<td>Last approvals granted (Shop)</td>
<td>Shows the last approvals granted for requests.</td>
</tr>
<tr>
<td>New requests</td>
<td>Shows new requests.</td>
</tr>
<tr>
<td>Number of requestable products</td>
<td>Shows the number of products that can be requested.</td>
</tr>
<tr>
<td>Denied requests by service category</td>
<td>Shows denied requests by service category.</td>
</tr>
<tr>
<td>Average request processing time by shop</td>
<td>Show the average processing time of a request by shop.</td>
</tr>
<tr>
<td>Top 10 requested products by shop</td>
<td>Shows the top 10 requested products by shop. This statistic is also available for the top 10 requested products by product owner.</td>
</tr>
<tr>
<td>Request frequency (12 months)</td>
<td>Shows the frequency of requests within the last 12 months.</td>
</tr>
</tbody>
</table>
Statistics

This statistic is also available for the frequency of requests within the last 12 months by owner.

For more information, see Departments on page 181.

Attestations

There are a number of statistics available to you for attestation cases. The following statistics are available.

Table 101: Attestation case statistics

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending attestation cases</td>
<td>Displays all open attestation cases. This statistic contains other criteria.</td>
</tr>
<tr>
<td></td>
<td>• By policy</td>
</tr>
<tr>
<td></td>
<td>• By next approver</td>
</tr>
<tr>
<td></td>
<td>• By framework</td>
</tr>
<tr>
<td>Attestation approval rates</td>
<td>Shows the approval rate for attestation.</td>
</tr>
<tr>
<td>Decided attestation approvals</td>
<td>Shows attestation approvals decisions within/over the limit.</td>
</tr>
<tr>
<td>within/over the limit</td>
<td>This statistic is also available for pending attestation cases within/over the limit.</td>
</tr>
<tr>
<td>Attestation status by type</td>
<td>Show attestation status by type.</td>
</tr>
<tr>
<td>Attestations</td>
<td>Shows all attestations.</td>
</tr>
<tr>
<td>Last approvals (attestation)</td>
<td>Shows the most recent attestation approval decisions.</td>
</tr>
<tr>
<td></td>
<td>This statistic is also available for attestations that have been granted approval.</td>
</tr>
<tr>
<td>Overdue attestations</td>
<td>Displays overdue attestations.</td>
</tr>
</tbody>
</table>

Target systems

There are a number of statistics available to you for target systems. The following statistics are available.
### Table 102: Target system statistics

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending attestation by system entitlements</td>
<td>Shows pending attestation by system entitlements.</td>
</tr>
<tr>
<td>Number of user accounts with a risk index of more than {0}</td>
<td>Shows the number of user accounts with a risk index more than specified value. This statistic is also available for the number of entitlements with a risk index more than specified value.</td>
</tr>
<tr>
<td>User accounts having risk higher {0} by domain</td>
<td>Shows user accounts with a risk index more than specified value by domain. This statistic contains other criteria.</td>
</tr>
<tr>
<td>Employees without user accounts</td>
<td>Show employees without user accounts.</td>
</tr>
<tr>
<td>Entitlements without requests</td>
<td>Shows entitlements without a request. This statistic contains other criteria.</td>
</tr>
<tr>
<td>Groups with / without user account assignments</td>
<td>Shows groups with or without user account assignments. This statistic contains other criteria.</td>
</tr>
<tr>
<td>Inactive employees with enabled</td>
<td>Shows inactive employees with enabled user.</td>
</tr>
</tbody>
</table>

- **Active Directory**
- **Oracle E-Business Suite**
- **LDAP**
- **SAP R/3**
- **SharePoint**
- **Notes**
- **Groups, roles and profiles with/without user account assignments SAP R/3**
<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user accounts</td>
<td>accounts.</td>
</tr>
<tr>
<td>Locked user accounts of enabled employees</td>
<td>Shows locked user accounts of active employees.</td>
</tr>
</tbody>
</table>
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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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
2
2FA 55

A
account
  new 14
address book 31
display 31
application roles 186
  add member 191
  attestation 195
  attestation approval decision 198
  attestation case approval
decision 198
  authorizations 193
  compliance 194
  compliance report 205
  create 187
delete member 192
display permissions 193
edit master data 190
history 201
master data 188
membership 190
remove member 192
risk index 199
role membership 204
rule violation 194
send reminder 197
show attestation 197
show attestation case 197
show attester 197
show compliance report 206
show history 202
show information 188
show master data 190
show member 191
show risk index 200
show role membership 204
show rule violation 195
show usage 204
usage 204
approval history
  view 96
attestation
  application roles 195
  execute 111
  managing attestation policies 114
  viewing completed attestations 109
auditing
  attestation 123
  employee details 230
  requests 98
  rule and policy violation 132
authentication 55

B
business roles
  edit master data 168
  manage 165
C
change
  security key 57
compliance
  application roles 194
  compliance admin 133
compliance framework
  viewing compliance frameworks 136
compliance report
  application roles 205
contact data
  rework 52
create
  security key 57
  user account 14

D
date format 54
delegation history
  call 220-221
delete
  security key 58
delete security key 58
display
  security key 56

E
edit
  security key 57
edit security key 57
employees
  add 144
  edit 144

F
fido 55
first login 14

H
header 20
history
  application roles 201
home page 20

K
key 55

L
language
  change 54
log in 14-15
  Password Reset Portal 16
  security key 16, 57
log out 14, 18
login 15

M
menu bar 21
my responsibilities
  manage 143

N
navigate 18
new
  account 14
security key 57
user account 14
number format 54

O
organization structure
manage 181
other services
edit master data 168

P
PAG 68
PAM 68
password 48, 50
change 50
password question 48
change 48
create 48
delete 48
edit 48
manage 48
specify 48
unlock 48
Password Reset Portal
log in 16
pending question
answer 97
privileged access 68

R
remove
security key 58
request
privileged access 68
request templates
create 73
edit 73
requests
act 62
about a reference user 64
for other recipient 65
from template 63
edit pending request 86
extend 72
manage 60
process monitoring 70
repeat 70
request email notification 247
request group 82
revoke 72
shopping cart aid 76
special request 82
responsibility
application roles 186
risk assessment
modifying risk calculators 135
risk index
application roles 199
role membership
application roles 204
roles
delegate 218
rule analysis 138
rule and policy violation
edit pending violations 130
view reports about rule and policy violation 137
rule violation
application roles 194
S
security 55
security key 55
    change 57
    create 57
log in 16
new 57
register 57
remove 58
set up 57
serve 18
setup
    security key 57
show security key 56
structure 19
system entitlements
    manage 158
system roles
    edit master data 168
    manage 165

T
two-factor authentication 55

U
usage
    application roles 204
user account
    create 14
    new 14
user interface 19

V
value format 54

W
W3C 55
WebAuthn 16, 55-58
white pages 31
display 31