



One Identity Manager 9.2

Web Portal User Guide

Copyright 2023 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/trademark-information.aspx. All other trademarks are the property of their respective owners.

Legend

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

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

One Identity Manager Web Portal User Guide
Updated - 12 October 2023, 13:13

For the most recent documents and product information, see [Online product documentation](#).

Contents

General tips and getting started	20
Logging in and out	21
Creating a new user account	21
Logging in	22
Logging in to the Password Reset Portal	22
Logging out	24
Navigation and use	24
Simple navigation	24
Search	26
Context searching	27
Help	27
Using the help	27
Filtering	27
Custom filter conditions	28
Displaying the address book	30
Changing the user interface theme	30
Managing password questions	30
Creating password questions	31
Editing password questions	31
Deleting password questions	32
Changing passwords	32
Editing your profile information	33
Switching languages	34
Enabling/disabling email notifications	34
Report subscriptions management	35
Subscribing to reports	35
Editing report subscriptions	36
Sending reports from report subscriptions	37
Unsubscribing reports	37
The user interface layout	38
Home	38

Header	39
Menu bar	39
Managing reports	40
Generating reports	40
Editing reports	42
Disabling/Enabling reports	43
Deleting reports	44
Generating reports	44
Requests	45
Setting up and configuring request functions	46
Managing shops	46
Displaying shops	47
Creating shops	47
Editing shops	48
Deleting shops	56
Managing service categories	56
Displaying service categories	56
Creating service categories	57
Editing service categories	59
Deleting service categories	61
Managing service items	61
Displaying service items	62
Editing service items	62
Managing product bundles	65
Displaying product bundles	66
Creating product bundles	67
Editing product bundles	68
Sharing product bundles	70
Deleting product bundles	71
Requesting products	71
Adding products to the shopping cart	72
Managing products in the shopping cart	73
Displaying the shopping cart	74
Removing products from the shopping cart	74

Setting the validity period of products in your shopping cart	75
Specifying the priority of products in your shopping cart	76
Giving reasons for requests	76
Checking the shopping cart	77
Requesting products in the shopping cart for multiple identities	77
Deleting shopping carts	78
Submitting requests	78
Requesting for other identities or subidentities	79
Displaying and requesting other identity's products	80
Requesting products through reference users	80
Requesting products through peer groups	81
Requesting using product bundles	82
Requesting privileged access	82
Requests for Active Directory groups	84
Requesting new Active Directory groups	84
Requesting changes to Active Directory groups	85
Requesting deletion of Active Directory groups	86
Requesting new SharePoint groups	87
Managing the Saved for Later list	88
Saving products for later	88
Displaying Saved for Later list	89
Requesting products on the Saved for Later list	89
Removing products from the Saved for Later list	90
Deleting the Saved for Later list	91
Pending requests	91
Displaying pending requests	91
Displaying pending request history	92
Displaying pending request entitlements	92
Displaying rule violations of pending requests	93
Approving and denying requests	93
Decision guidance for request approvals	94
Approving pending requests from newly created Active Directory groups	94
Approving pending requests from newly created SharePoint groups	96
Approving new managers' pending requests	96
Appointing other approvers for pending requests	97

Rerouting approvals of pending requests	98
Appointing additional approvers to pending requests	99
Delegating approvals of pending requests to other identities	100
Escalating approvals of pending requests	102
Rejecting request approval	102
Managing inquiries about pending requests	103
Sending inquiries about pending requests	103
Recalling inquiries about pending requests	104
Canceling reservations of pending requests	104
Displaying answers to inquiries about pending requests	105
Displaying request history	105
Canceling requests	106
Renewing products with limit validity periods	107
Unsubscribing products	108
Displaying requests	110
Undoing approvals	110
Managing request inquiries directed at you	111
Displaying request inquiries	111
Answering inquiries about requests	111
Attestation	113
Managing attestations	113
Attestation policy settings	114
Displaying attestation policies	114
Displaying attestation policy reports	115
Setting up attestation policies	116
Editing attestation policies	118
Copying attestation policies	121
Deleting attestation policies	124
Starting attestation	124
Running sample attestations	125
Managing attestation runs	126
Displaying attestation policy runs	127
Extending attestation runs	129
Attestation by peer group analysis	129
Managing samples	130

Displaying samples	130
Creating samples	130
Editing samples	131
Deleting samples	131
Sending attestation reminders	132
Sending reminders about attestation runs	132
Grouping attestation policies (using policy collections)	132
Displaying policy collections	133
Creating policy collections	133
Editing policy collections	134
Disabling policy collections	135
Deleting policy collections	136
Assigning policy collections to attestation policies	136
Pending attestations	136
Displaying pending attestation cases	137
Approving or denying attestation cases	138
Appointing other approvers for pending attestation cases	139
Rerouting approvals of pending attestation cases	139
Appointing additional approvers to pending attestation cases	140
Delegating approvals of pending attestation cases to other identities	142
Rejecting approval of attestation cases	144
Managing inquiries about pending attestation cases	145
Submitting inquiries about pending attestation cases	146
Withdrawing inquiries about pending attestation cases	146
Revoking reserved attestation cases	147
Displaying answers to inquiries about pending attestation cases	147
Displaying attestation history	148
Managing attestation inquiries directed at you	149
Displaying attestation case inquiries	149
Answering attestation case inquiries	149
Compliance	151
Managing compliance rules	151
Displaying compliance rules	152
Displaying rule violations of compliance rules	152
Displaying mitigating controls of compliance rules	153

Displaying compliance rule statistics	153
Displaying compliance rule hyperviews	154
Displaying reports about compliance rules and rule violations	154
Check compliance rules and find rule violations	155
Managing rule violations	155
Displaying approvable rule violations	155
Assigning mitigating controls to rule violations	156
Granting and denying rule violation exceptions	156
Resolving rule violations	157
Managing company policies	158
Displaying company policies	158
Displaying policy violations of company policies	159
Displaying mitigating controls of company policies	160
Displaying company policy statistics	160
Displaying company policy hyperviews	160
Managing policy violations	161
Displaying approvable policy violations	161
Assigning mitigating controls to policy violations	161
Granting and denying policy violation exceptions	162
Managing risk index functions	163
Displaying risk index functions	164
Editing risk index functions	164
Disabling/enabling risk index functions	166
Starting risk index calculation manually	166
Responsibilities	168
My responsibilities	168
Managing my departments	169
Displaying my departments	170
Creating your own departments	170
Displaying and editing my department main data	171
Copying/splitting my departments	173
Comparing and merging my departments	175
Restoring my departments to their previous state	176
Managing my department memberships	176

Managing my departments' entitlements	180
Displaying my departments' rule violations	181
My departments' history	182
Restoring my deleted departments	183
Managing my application roles	184
Displaying my application roles	184
Creating your own application roles	184
Displaying and editing my application roles' main data	186
Restoring my application roles to their previous state	187
Managing my application role memberships	188
Displaying my application roles' rule violations	192
My application roles' history	192
Managing my devices	193
Displaying my devices	194
Creating your own devices	194
Displaying and editing my devices' main data	196
Deleting your own devices	199
Managing my business roles	199
Displaying my business roles	200
Creating your own business roles	200
Displaying and editing my business roles' main data	202
Copying/splitting my business roles	204
Comparing and merging my business roles	205
Restoring my business roles to their previous state	206
Managing my business role memberships	207
Managing my business roles' entitlements	210
Displaying my business roles' rule violations	212
My business roles' history	212
Restoring my deleted business roles	214
Managing my identities	214
Displaying my identities	215
Creating your own identities	216
Comparing my identities	219
Displaying and editing my identities' main data	220
Displaying my identities' risk indexes	222

Deactivating my identities	222
Marking my identities as security risks	223
Assigning other managers to my identities	224
Creating passcodes for my identities	225
Creating reports about my identities	225
Managing my identities' memberships	226
Displaying identities' organizational charts	230
My identities' history	230
Displaying my identity requests	232
Managing my identities' attestation cases	232
Displaying my identities' rule violations	234
Managing my cost centers	234
Displaying my cost centers	235
Creating your own cost centers	235
Displaying and editing my cost center main data	236
Copying/splitting my cost centers	238
Comparing and merging my cost centers	239
Restoring my cost centers to their previous state	240
Managing my cost center memberships	241
Managing my cost centers' entitlements	244
Displaying my cost center rule violations	246
My cost center history	246
Restoring my deleted cost centers	248
Managing my multi-request resources	248
Displaying my multi-request resources	249
Displaying and editing my multi-request resources' main data	249
Managing my multi requestable/unsubscribable resources	250
Displaying my multi requestable/unsubscribable resources	251
Displaying and editing my multi requestable/unsubscribable resources' main data	251
Managing my resources	252
Displaying my resources	253
Displaying and editing my resources' main data	253
Managing my software applications	254
Displaying my software applications	254

Displaying and editing my software applications' main data	255
Displaying my software application owners	257
Managing my software application memberships	257
Managing service items of my software applications	259
Managing my locations	263
Displaying my locations	264
Creating your own locations	264
Displaying and editing my locations' main data	265
Copying/splitting my locations	267
Comparing and merging my locations	268
Restoring my locations to their previous state	269
Managing my location memberships	270
Managing my locations' entitlements	273
Displaying my locations' rule violations	275
My locations' history	275
Restoring my deleted locations	277
Managing my system entitlements	277
Displaying my system entitlements	278
Displaying and editing my system entitlements' main data	278
Creating reports about my system entitlements	279
Making my system entitlements requestable	280
Specifying my system entitlement owners	280
Managing my system entitlements' service items	281
Managing my system entitlement memberships	285
Managing my system entitlements' child groups	287
My system entitlements' history	288
Managing my system entitlements' attestation cases	290
Managing my system roles	292
Displaying my system roles	292
Creating your own system roles	292
Displaying and editing my system roles' main data	294
Managing my system role memberships	295
Managing my system roles' entitlements	298
Displaying my system roles' rule violations	299
My system roles' history	300

Managing my assignment resources	301
Displaying my assignment resources	302
Displaying and editing my assignment resource main data	302
Managing task delegations	303
Displaying delegations	304
Creating delegations	304
Canceling delegations	305
Deleting delegations	305
Ownerships	306
Assigning owners to system entitlements	306
Assigning owners to devices	307
Managing data	308
Managing departments	309
Displaying departments	309
Creating departments	309
Displaying and editing department main data	312
Copying/splitting departments	314
Comparing and merging departments	315
Restoring departments to their previous state	316
Managing department memberships	317
Displaying department memberships	317
Analyzing assignments to departments	318
Adding identities to departments	318
Removing identities from departments	320
Managing department entitlements	320
Displaying department entitlements	321
Adding entitlements to departments	321
Deleting department entitlements	322
Displaying department rule violations	322
Department history	322
Displaying department history	323
Displaying the status overview of departments	323
Comparing statuses of departments	324
Restoring deleted departments	324
Managing user accounts	324

Displaying user accounts	325
Editing user accounts	325
Managing user account memberships	326
Displaying user account memberships	326
Creating reports about user accounts	326
Managing business roles	327
Displaying business roles	327
Creating business roles	327
Displaying and editing business role main data	330
Copying/splitting business roles	332
Comparing and merging business roles	333
Restoring business roles to their previous state	334
Managing business role memberships	335
Displaying business role memberships	335
Analyzing assignments to business roles	336
Assigning identities to business roles	336
Removing business roles from identities	338
Managing business role entitlements	338
Displaying business role entitlements	339
Adding entitlements to business roles	339
Deleting business role entitlements	340
Displaying business role rule violations	340
Business role history	340
Displaying business role history	341
Displaying the status overview of business roles	341
Comparing statuses of business roles	342
Restoring deleted business roles	342
Managing identities	342
Displaying identities	343
Displaying and editing identity main data	343
Creating identities	345
Comparing identities	348
Displaying and analyzing identities' risk indexes	349
Deactivating identities	350
Reactivating identities	350

Marking identities as security risks	350
Revoking identities' security risks	351
Deleting identities	351
Assigning other managers to identities	352
Creating reports about identities	352
Managing identities' memberships	353
Analyzing identities' membership assignments	354
Displaying identities' departments	354
Displaying identities' application roles	354
Displaying identities' user accounts	355
Displaying identities' business roles	355
Displaying identities' cost centers	355
Displaying identities' shops	356
Displaying identities' locations	356
Displaying identities' system entitlements	356
Displaying identities' system roles	357
Displaying identities' organizational charts	357
Identity history	357
Displaying identities' history	358
Displaying the status overview of identities	358
Comparing statuses of identities	359
Managing attestation cases of identities	359
Displaying attestation cases of identities	359
Approving and denying attestation cases of identities	360
Displaying identities' rule violations	361
Managing cost centers	361
Displaying cost centers	362
Creating cost centers	362
Displaying and editing cost center main data	363
Copying/splitting cost centers	365
Comparing and merging cost centers	366
Restoring cost centers to their previous state	367
Managing cost center memberships	368
Displaying cost center memberships	368
Analyzing assignments to cost centers	369

Adding identities to cost centers	369
Removing identities from cost centers	371
Managing cost center entitlements	371
Displaying cost center entitlements	372
Adding entitlements to cost centers	372
Deleting cost center entitlements	373
Displaying cost center rule violations	373
Cost center history	373
Displaying cost center history	374
Displaying the status overview of cost centers	374
Comparing statuses of cost centers	375
Restoring deleted cost centers	375
Managing multi-request resources	375
Displaying multi-request resources	376
Displaying and editing multi-request resources main data	376
Managing multi requestable/unsubscribable resources	377
Displaying multi requestable/unsubscribable resources	377
Displaying and editing multi requestable/unsubscribable resource main data	378
Managing resources	379
Displaying resources	380
Displaying and editing resource main data	380
Managing locations	381
Displaying locations	382
Creating locations	382
Displaying and editing location main data	383
Copying/splitting locations	385
Comparing and merging locations	386
Restoring locations to their previous state	387
Managing location memberships	388
Displaying location memberships	388
Analyzing assignments to locations	388
Adding identities to locations	389
Removing identities from locations	391
Managing location entitlements	391
Displaying location entitlements	391

Adding entitlements to locations	392
Deleting entitlements from locations	392
Displaying location rule violations	393
Location history	393
Displaying location history	394
Displaying the status overview of locations	394
Comparing statuses of locations	394
Restoring deleted locations	395
Managing system entitlements	395
Displaying system entitlements	396
Making system entitlements requestable	396
Displaying and editing system entitlements main data	397
Specifying system entitlement owners	398
Managing service items for system entitlements	400
Creating service items for system entitlements	400
Editing system entitlement service items	404
Managing system entitlement memberships	407
Displaying system entitlement memberships	408
Analyzing assignments to system entitlements	408
Assigning identity system entitlements	408
Removing system entitlements from identities	409
Managing system entitlement child groups	409
Displaying system entitlements' child groups	410
System entitlement history	410
Displaying system entitlement history	411
Displaying the status overview of system entitlements	411
Comparing statuses of system entitlements	411
Managing attestation cases of system entitlements	412
Displaying attestation cases of system entitlements	412
Approving and denying attestation cases of system entitlements	413
Creating reports about system entitlements	413
Managing system roles	414
Displaying system roles	414
Creating system roles	414
Displaying and editing system role main data	416

Managing system role memberships	417
Displaying system role memberships	418
Analyzing assignments to system roles	418
Assigning identities to system roles	418
Removing identities from my system roles	419
Managing system role entitlements	420
Displaying system role entitlements	420
Adding entitlements to system roles	420
Deleting system role entitlements	421
Displaying system role rule violations	421
System role history	422
Displaying system role history	422
Displaying the status overview of system roles	422
Comparing statuses of system roles	423
Managing assignment resources	423
Displaying assignment resources	423
Displaying and editing assignment resource main data	424
Opening other web applications	425
Managing tickets	426
Display tickets	426
Displaying ticket history	426
Creating tickets	427
Editing tickets	427
Managing ticket attachments	428
Displaying ticket attachments	429
Attaching files to tickets	429
Downloading ticket attachments	429
Creating folders for ticket attachments	430
Deleting ticket attachments and folders	430
Appendix: Attestation conditions and approval policies from attestation procedures	431
Attesting primary departments	431
Attesting primary business roles	432
Attesting primary cost centers	433

Attesting primary locations	433
Attesting secondary departments	434
Attesting secondary cost centers	435
Attesting secondary locations	435
Attesting PAM asset groups	436
Attesting PAM asset accounts	436
Attesting PAM assets	437
Attesting PAM user groups	437
Attesting PAM user accounts	438
Attesting PAM account groups	439
Attesting PAM directory accounts	439
Attesting PAM accesses	440
Attesting departments	441
Application role attestation	442
Business role attestation	442
Attesting system roles	443
Attesting locations	444
Attesting system roles	445
Attesting memberships in system entitlements	446
Attesting memberships in application roles	448
Attestation of memberships in business roles	450
Attesting assignment of memberships in system roles	451
Attesting device owners	453
Attesting system entitlement owners	453
Attesting system entitlement owners (initial)	453
Attesting user accounts	454
Attesting system entitlements	455
Attesting assignment of system entitlement to departments	456
Attesting assignment of system entitlement to business roles	458
Attestation of system entitlement assignments to cost centers	459
Attestation of system entitlement assignments to locations	460
Attesting assignment of system role assignment to departments	461
Attesting assignment of system roles to business roles	462
Cost center system role assignment attestation	464
Attesting assignment of system entitlements to locations	465

Attesting assignments to system roles	466
About us	467
Contacting us	467
Technical support resources	467
Index	468

General tips and getting started

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

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

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

Tips for using the Web Portal

- Enable JavaScript in your browser for the Web Portal to work.
- For optimal displaying of the graphical user interface, use a device with a minimum screen resolution of 1280 x 1024 pixels and at least 16-bit color depth. For mobile viewing, for example when using a tablet, use a device with a display size of at least 9.7 inches.
- Supported browsers:
 - Firefox (release channel)
 - Chrome (release channel)
 - Safari (current version)
 - Microsoft Edge (release channel)

Detailed information about this topic

- [Logging in and out](#) on page 21
- [Navigation and use](#) on page 24
- [Displaying the address book](#) on page 30
- [Changing the user interface theme](#) on page 30
- [Managing password questions](#) on page 30

- [Changing passwords](#) on page 32
- [Switching languages](#) on page 34
- [Enabling/disabling email notifications](#) on page 34
- [Report subscriptions management](#) on page 35
- [The user interface layout](#) on page 38

Logging in and out

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

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

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

Detailed information about this topic

- [Creating a new user account](#) on page 21
- [Logging in](#) on page 22
- [Logging in to the Password Reset Portal](#) on page 22
- [Logging out](#) on page 24

Creating a new user account

To log in to the Web Portal, you need a user account. If you do not already have a user account, you will have to create a new one.

To create a new user account

1. In your web browser, enter the web address (URL) of the Password Reset Portal.
2. Click **Create new account** on the login page.
3. In the **Create New Account** pane, enter your data (at least **Last name**, **First name**, and **Contact email address**).
4. In the **Enter characters from the image** field, enter the Captcha Code displayed.

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

5. Click **Create account**.

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 email address**.
8. Define your password and your password questions (see [Changing passwords](#) on page 32 and [Managing password questions](#) on page 30).
9. You can then log in using these credentials (see [Logging in](#) on page 22).

Related topics

- [Changing passwords](#) on page 32
- [Managing password questions](#) on page 30

Logging in

Open the Web Portal in a web browser.

To log in to the Web Portal

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

Related topics

- [Changing passwords](#) on page 32

Logging in to the Password Reset Portal

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

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

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

To log in to Password Reset Portal using an passcode

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

To log in to Password Reset Portal using your password questions

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

To log in to Password Reset Portal using your current password

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

Related topics

- [Logging in](#) on page 22
- [Logging out](#) on page 24

Logging out

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

To log off from Web Portal

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

Your logout was successful.

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

Navigation and use

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

Detailed information about this topic

- [Simple navigation](#) on page 24
- [Search](#) on page 26
- [Help](#) on page 27
- [Filtering](#) on page 27

Simple navigation

Simple commands

Table 1: Overview of simple commands

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

NOTE: Take into account that not all browsers behave the same.

Go to the home page

Table 2: Overview of key combinations for navigating

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

Simple elements

Table 3: Overview of the controls used

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

Installed controls

Table 4: Overview of other controls

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

Search

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

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

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

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

Example	Description
Sam User	Finds Sam User but not Sam Identity. Search results must contain all of the separate terms in the query. A logical AND is used.
Sam OR Identity	Finds Sam User and Pat Identity. Placing OR between the search terms acts as a logical OR operator. The results of this search contain at least one of the two search terms.
Sam NOT User	Finds Sam Identity but not Sam User. The results of this search do not contain the term that comes after NOT .
U*	Finds User1 and User2. The * functions as a wildcard for any number of characters to complete the term.
Use?	Finds User but not User1. The ? functions as a wildcard for a single character to complete the term.
"Sam User"	Provides results in which the search terms Sam and User follow one another. Results of this search contain the string in quotes as phrase.
Sam User~	Finds Sam User and also other similar results. A tilde ~ after the search term indicates that the search should also find similar results. This means that incorrectly spelled terms can be found, as well. You can specify the level of similarity by adding a number between 0 and 1 (with decimal point) after the tilde ~. The higher the number, the more similar the results.

Detailed information about this topic

- [Context searching](#) on page 27

Context searching

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

To run a context search

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

Help

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

Detailed information about this topic

- [Using the help](#) on page 27

Using the help

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

To call up help in the Web Portal

- In the header, click ? (**Help**) > **Documentation**.

Filtering

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

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

To use a filter

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

Detailed information about this topic

- [Custom filter conditions](#) on page 28

Custom filter conditions

In some places in the Web Portal you can create custom filter conditions.

The wizard is available to you at different places in the Web Portal.

To use the wizard, first select a property then specify a comparison operator and a comparison value.

Comparison operators

You can use the following operators to define a condition. The type of comparison operator depends on the selected property.

Table 6: Comparison operators

Value type	Operator	Description
Text value	is equal to	Finds the same text value.
	precedes the word in the alphabet	Finds all results that occur before the entered text in alphabetical order.
	follows the word in the alphabet	Finds all results that occur after the entered text in alphabetical order.
	not equal	Finds all results that are not the same as the entered text.
	is contained in	Finds all results that include one of the given text values. Click Add new value to add another value.
	contains	Finds all results that contain the text value.
	starts with	Finds all results that begin with the entered text value.
	ends with	Finds all results that end with the entered text value.
	is equal or precedes the word in the alphabet	Finds all results that either contain the entered text value or occur before the entered text value in alphabetical order.
	is equal or follows the word in the alphabet	Finds all results that either contain the entered text value or occur after the entered text value in alphabetical order.

Value type	Operator	Description
Numerical value	is less than	Finds all results that are smaller than the entered numerical value.
	is greater than	Finds all results that are larger than the entered numerical value.
	is equal to	Finds all results that are the same as the entered numerical value.
	is less or equal	Finds all results that are less than or equal to the entered numerical value.
	is greater than or equal	Finds all results that are greater than or equal to the entered numerical value.
	not equal	Finds all results that are not the same as the entered numerical value.
Date value	older than	Finds all results that are older than the given date.
	younger than	Finds all results that are younger than the given date.
	is equal to	Finds all results that are the same as the given date.
	older than or equal to	Finds all results that are greater than or equal to the given date.
	younger than or equal to	Finds all results that are younger than or equal to the given date.
	is not equal to	Finds all results that are not the same as the given date.
Boolean value	Property is activated	<p>If the switch is set, all results are searched for where this property is enabled.</p> <p>If the switch is not set, all results are searched for where this property is disabled.</p>

Comparison values

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

You can enter date values as relative (in hours, days, months, or years) but also as absolute values (fixed date).

Boolean values

Set the switch to display all data sets with this property is enabled.

Do not set the switch to display all data sets with this property is disabled.

Link conditions

To link conditions you can use the logical operators AND and OR.

Displaying the address book

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

To display the address book

1. In the header, click  (**Profile**) > **Address Book**.
This displays the address book and all identities.
2. (Optional) On the **Address Book** page, click an identity.
In the **Edit Identity Data** pane, there are further details about the identity.

Changing the user interface theme

You change the appearance of the Web Portal user interface by changing the theme. For example, you can use a contrasting theme.

To change the theme of the user interface

1. In the header, click  (**Profile**) > **Themes**.
2. In the **Themes** dialog, select the theme you want in the **Application theme** menu.
TIP: The **Device theme** theme takes the theme from your operating system.
3. Click **Close**.

Managing password questions

If you forget your password, you can change it at any time in the Web Portal (see [Changing passwords](#) on page 32). To do this, you need to define individual questions that only you can answer.

If your password questions are answered incorrectly several times, they may be locked (depending on the system configuration).

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

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

Detailed information about this topic

- [Creating password questions](#) on page 31
- [Editing password questions](#) on page 31
- [Deleting password questions](#) on page 32

Creating password questions

You can create new password questions.

To create new a password question

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page click the **Password Questions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Password Questions** tab, click **+ Create password question**.
5. In the **Create Password Question** pane, enter the following:
 - **Question:** Enter your question.
 - **Answer:** Enter the answer to your question (above).
 - **Repeat answer:** Enter the answer to your question again.
6. Click **Save**.

Editing password questions

You can edit existing password questions.

To edit a password question

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page click the **Password Questions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. In the **Password Questions** tab, click the password question you want to edit.
5. In the **Edit Password Question** pane, enter the following:

- **Question:** Enter your question.
 - **Answer:** Enter the answer to your question (above).
 - **Repeat answer:** Enter the answer to your question again.
6. Click **Save**.

Deleting password questions

You can delete existing password questions.

To delete a password question

1. In the header, click **Profile** > **Profile**.
2. On the **Profile Settings** page, click the **Password Questions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Password Questions** tab, enable the check box in front of the password question you want to delete.
5. Click **Delete**.
6. In the **Delete password question** dialog, confirm the prompt with **Yes**.

Changing passwords

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

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

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

Step 1: Log in to the Password Reset Portal

Log in to the Password Reset Portal using a passcode, by answering your password questions, or with your current password (see [Logging in to the Password Reset Portal](#) on page 22).

Step 2: Change password

After you have logged in on the Password Reset Portal (see [Step 1: Log in to the Password Reset Portal](#) on page 32), you can change your central password or the passwords of user accounts to which you have access.

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

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

To change the central password

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

The central password is reset.

Related topics

- [Managing password questions](#) on page 30

Editing your profile 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 **👤 (Profile) > Profile**.
2. On the **Profile Settings** page, click the **Password Questions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.

| NOTE: Changes to your contact data only affects the selected identity.

4. Edit the entries in the various fields.
5. (Optional) To change your profile picture, perform the following actions:

- a. Click **Add/Change**.
 - b. Select an image from your medium.
6. Click **Save**.

Switching languages

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

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

NOTE: Your system might be configured to use the language that your browser always uses. In this case, the configuration described in the following only applies to emails the Web Portal sends.

To change the language of the Web Portal

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page, click the **Password Questions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. In the **Language** menu, select the language that you want to use for the Web Portal.
5. In the **Language for value formatting** menu, select the language you want to use for date and number formats.

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

6. Click **Save**.

Enabling/disabling email notifications

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

To enable/disable email notifications

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page, click the **Email Notifications** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Email Notifications** tab, perform one of the following actions:

- To enable notifications, select the check box next to the event you want to be notified about.
- To disable notifications, deselect the box next to the event you do not want to be notified about anymore.

5. Click **Save**.

Report subscriptions management

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

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

For more information about report subscriptions, see the *One Identity Manager Report Subscriptions Administration Guide*.

Detailed information about this topic

- [Subscribing to reports](#) on page 35
- [Editing report subscriptions](#) on page 36
- [Sending reports from report subscriptions](#) on page 37
- [Unsubscribing reports](#) on page 37
- [Managing reports](#) on page 40

Subscribing to reports

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

To add a subscription

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Report Subscriptions** tab, click **+ Add subscription**.
5. In the **Add Report Subscription** pane, click the report that you want to subscribe to.

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

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

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

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

Editing report subscriptions

You can edit your existing report subscriptions.

To edit a report subscription

1. In the header, click **👤 (Profile) > Profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Report Subscriptions** tab, click the report subscription that you want to edit.
5. In the **Subscription Details** pane, configure the following report subscription settings:

- **Subscription:** Enter the report subscription's name.
- **Report:** Select the report that you want to subscribe to.
- **Schedule:** Select how often you want to receive the report (once a week, for example).
- **Format (email attachment):** Select which format you want to receive the report in. The report is sent in this format as a file attachment in an email.
- **Additional subscribers:** Click **Select/Change**, select the check box next to the identity who will also receive this report and click **Apply**.

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

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

Sending reports from report subscriptions

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

To send a report

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.
3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Report Subscriptions** tab, perform the following:
 - To send the report, click  **Actions** > **Send report to me** next to the subscription of the report that you want to send.
 - To send the report to all subscribers, click  **Actions** > **Send report to all subscribers** next to the subscription of the report you want to send.

Unsubscribing reports

You can unsubscribe reports.

To unsubscribe a report

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.

3. (Optional) If you have other subidentities besides your main identity, you can select identities from the **Identity** menu.
4. On the **Report Subscriptions** tab, click **⋮ Actions > Unsubscribe** next to the report subscription that you want to end.
5. In the **Unsubscribe Report** dialog, confirm the prompt with **OK**.

The user interface layout

The Web Portal user interface is divided into several sections:

Top - header

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

Top – menu bar

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

Work area

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

Detailed information about this topic

- [Home](#) on page 38
- [Header](#) on page 39
- [Menu bar](#) on page 39

Home

Open the home page by clicking the company logo.

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

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

Header

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

Table 7: Functions in the header

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

Menu bar

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

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

To open a menu

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

Managing reports

Reports contain information about objects and their relations to other database objects. Identification, analysis, and summaries of relevant data are supported with the help of these reports.

You can display, create, and edit reports. You and other Web Portal users can subscribe to these reports.

For more information about reports, see the *One Identity Manager Report Subscriptions Administration Guide*.

Related topics

- [Report subscriptions management](#) on page 35

Detailed information about this topic

- [Generating reports](#) on page 40
- [Editing reports](#) on page 42
- [Disabling/Enabling reports](#) on page 43
- [Deleting reports](#) on page 44
- [Generating reports](#) on page 44

Generating reports

In the default installation there are predefined reports available that you can subscribe to in the Web Portal. You can also create your own reports.

To generate a report

1. In the menu bar click **Setup > Reports**.
2. On the **Reports** page, click **+ Create report**.
3. In the **Create Report** pane, enter the new report's main data.

You can edit the following main data.

Table 8: Report main data

Property	Description
Name	Enter the report's name.
Description	Enter a description for the report.
Risk index	Use the slider to define the report's risk index.
Disabled	Select the check box if you want to the report to be disabled (see Disabling/Enabling reports on page 43). Only subscribable reports that are enabled can be assigned within One Identity Manager. If a report is disabled, you are prevented from assigning the subscribable report. Existing assignments remain intact. IMPORTANT: If you disable a subscribable report, existing Web Portal user report subscriptions are canceled.
Owners	Select the identity that is responsible for this report. This identity can view and edit the report.
Available to	Click Select/Change and select the identities that can call up this report and subscribe to it.

4. In the **Include data from the table** menu, select the base table whose content you want to include in the report.
5. Specify which information to include in the report. Then enter which columns of the base table to add to the report:
 - a. Under **Columns to be included**, click **Add column**.
 - b. In the menu, select the respective column.
 - c. (Optional) To add another column to the report, repeat this step.

| **TIP:** To remove a column, click  (**Delete**).

| **TIP:** Drag and drop the columns to change their order.
6. (Optional) To place further restrictions on the data in the report, set conditions. Perform the following actions as well:
 - a. Under **Conditions**, click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition to the report, repeat this step.

- f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

| **TIP:** To remove a condition, click  (**Delete**).

For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.

7. Click **Create**.

Editing reports

You can edit your own reports.

To edit a report

1. In the menu bar click **Setup > Reports**.
2. On the **Reports** page, click the report you want to edit.
3. In the **Edit Report** pane, edit the report's main data.

You can edit the following main data.

Table 9: Report main data

Property	Description
Name	Enter the report's name.
Description	Enter a description for the report.
Risk index	Use the slider to define the report's risk index.
Disabled	Select the check box if you want to the report to be disabled (see Disabling/Enabling reports on page 43). Only subscribable reports that are enabled can be assigned within One Identity Manager. If a report is disabled, you are prevented from assigning the subscribable report. Existing assignments remain intact. IMPORTANT: If you disable a subscribable report, existing Web Portal user report subscriptions are canceled.
Owners	Select the identity that is responsible for this report. This identity can view and edit the report.
Available to	Click Select/Change and select the identities that can call up this report and subscribe to it.

4. In the **Include data from the table** menu, select the base table whose content you want to include in the report.

5. Specify which information to include in the report. Then enter which columns of the base table to add to the report:
 - a. Under **Columns to be included**, click **Add column**.
 - b. In the menu, select the respective column.
 - c. (Optional) To add another column to the report, repeat this step.

| **TIP:** To remove a column, click  (**Delete**).

| **TIP:** Drag and drop the columns to change their order.

6. (Optional) To place further restrictions on the data in the report, set conditions. Perform the following actions as well:
 - a. Under **Conditions**, click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition to the report, repeat this step.
 - f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

| **TIP:** To remove a condition, click  (**Delete**).

For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.

7. Click **Save**.

Disabling/Enabling reports

You can disabled reports. Only subscribable reports that are enabled can be assigned within One Identity Manager. If a report is disabled, you are prevented from assigning the subscribable report. Existing assignments remain intact. To enable disabled reports again.

| **IMPORTANT:** If you disable a subscribable report, existing Web Portal user report subscriptions are canceled.

To disable an enabled report

1. In the menu bar click **Setup > Reports**.
2. On the **Reports** page, click the report you want to disable.
3. In the **Edit Report** pane, select the **Disabled** control box.
4. Click **Save**.

To enable a disabled report

1. In the menu bar click **Setup > Reports**.
2. On the **Reports** page, click the report you want to enable.
3. In the **Edit Report** pane, clear the **Disabled** control box.
4. Click **Save**.

Deleting reports

You can delete reports.

IMPORTANT: If you delete a subscribable report, existing Web Portal user report subscriptions are canceled.

To delete a report

1. In the menu bar click **Setup > Reports**.
2. On the **Reports** page, select the check box next to the report you want to delete.
3. Click  **Delete**.
4. In the **Delete Reports** dialog, confirm the prompt with **Yes**.

Generating reports

You can generate reports and display the collected data.

To generate a report

1. In the header, click  (**Profile**) > **Profile**.
2. On the **Profile Settings** page, click the **Report Subscriptions** tab.
3. On the **Report Subscriptions** tab, click **View a report**.
4. On the **View a Report** pane, click the report you want to generate.
5. In the **Format** menu, select the format to use to generate the report.
6. Click **Show report**.

This downloads the report.

Requests

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

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

You can apply the following requests:

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

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

- Your request is forwarded to an identity for approval (see [Pending requests](#) on page 91).
- You are notified whether your request is granted or denied.

Detailed information about this topic

- [Setting up and configuring request functions](#) on page 46
- [Requesting products](#) on page 71
- [Managing the Saved for Later list](#) on page 88
- [Pending requests](#) on page 91
- [Displaying request history](#) on page 105
- [Canceling requests](#) on page 106
- [Renewing products with limit validity periods](#) on page 107
- [Unsubscribing products](#) on page 108
- [Displaying requests](#) on page 110
- [Managing request inquiries directed at you](#) on page 111

Setting up and configuring request functions

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

Structure and workflow of requests

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

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

Requests follow a defined approval process that determines whether a product may be assigned or not. Authorized identities have the option to approve requests and cancellations. You determine which approval process to use by assigning approval policies to shops or shelves (see [Editing shop details](#) on page 48 and [Editing shelf details](#) on page 51).

Detailed information about this topic

- [Managing shops](#) on page 46
- [Managing service categories](#) on page 56
- [Managing service items](#) on page 61
- [Managing product bundles](#) on page 65

Managing shops

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

A shop can contain several shelves (see [Managing shop shelves](#) on page 49). Products are assigned to these shelves and can then be requested (see [Managing requestable products in shops](#) on page 54).

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

You can also decide who is able to request products from shops (see [Manage access to requestable products in Shops](#) on page 53).

Detailed information about this topic

- [Displaying shops](#) on page 47
- [Creating shops](#) on page 47
- [Editing shops](#) on page 48
- [Deleting shops](#) on page 56
- [Managing shop shelves](#) on page 49
- [Manage access to requestable products in Shops](#) on page 53
- [Managing requestable products in shops](#) on page 54

Displaying shops

You can display any of the shops and their details.

To display shops

1. In the menu bar click **Setup > Shops**.
This opens the **Shops** page.
2. (Optional) To display details of a shop, in the list, click on the shop.
3. (Optional) You can perform the following actions:
 - You can display the shop's shelves (see [Displaying shop shelves](#) on page 50).
 - You can display who can request products from the shop (see [Displaying members of shops](#) on page 53).

Creating shops

To set up your own shop solution, you can create shops. You can then customize these shops as you wish (see [Editing shops](#) on page 48).

To create a shop

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

Table 10: Shop main data

Property	Description
Name	Enter a full, descriptive name for the shop.

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

4. Click **Create**.
5. (Optional) Create shelves for the shop (see [Creating shelves for shops](#) on page 50). In the shelves, you can specify which products can be requested from the shop (see [Adding products to shelves](#) on page 55).
6. (Optional) To specify who can request products from the shop, add members to the shop (see [Adding members to shops](#) on page 53).

Editing shops

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

- Edit shop details (see [Editing shop details](#) on page 48)
- Manage shop shelves (see [Managing shop shelves](#) on page 49)
- Specify who can request products from shops (see [Manage access to requestable products in Shops](#) on page 53)
- Specify which products can be requested from shops (see [Managing requestable products in shops](#) on page 54)

Editing shop details

You can edit details of existing shops.

To edit details of a shop

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

Table 11: Shop main data

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

4. Click **Save**.

Managing shop shelves

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

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

Detailed information about this topic

- [Displaying shop shelves](#) on page 50
- [Creating shelves for shops](#) on page 50
- [Editing shop shelves](#) on page 51

- [Editing shelf details](#) on page 51
- [Deleting shop shelves](#) on page 52

Displaying shop shelves

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

To display the shelves in a store

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, in the list, click the shop whose shelves you want to display.
3. In the **Edit Shop** pane, click the **Shelves** tab.
4. (Optional) To display details of a shelf, click it in the list.
5. (Optional) You can display the products that can be requested over this shelf (see [Displaying requestable products](#) on page 54).

Creating shelves for shops

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

To create a shelf for shop

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

Table 12: Shelves main data

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

Property	Description
	This setting is inherited by all the products that are assigned to this shop and do not have any approval policies.
Owner	Select the identity that is responsible for the shelf. The owner can be used as the approver in approval processes for off the shelf requests.
Deputy manager	Select the identity that deputizes for the shelf manager. The deputy can be used as the approver in approval processes for off the shelf requests.

6. Click **Create**.
7. (Optional) To specify which products can be requested from the shelf, add the corresponding products to the shelf (see [Adding products to shelves](#) on page 55).

Editing shop shelves

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

- Edit shelf details (see [Editing shop details](#) on page 48)
- Specify which products can be requested from shops (see [Managing requestable products in shops](#) on page 54)

Editing shelf details

You can edit details of existing shelves.

To edit details of a shelf

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

- In the **Edit shelf** pane, you can edit the main data of the shelf.

Table 13: Shelves main data

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

- Click **Save**.

Related topics

- [Managing requestable products in shops](#) on page 54

Deleting shop shelves

You can delete shops.

NOTE: Before you can delete a shelf, you must remove all the products from it (see [Removing products from shelves](#) on page 55).

To delete a shelf from a shop

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

Manage access to requestable products in Shops

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

Detailed information about this topic

- [Displaying members of shops](#) on page 53
- [Adding members to shops](#) on page 53
- [Removing members from shops](#) on page 54

Displaying members of shops

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

To display members of a shop

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

Adding members to shops

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

To add a member to a shop

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

To add excluded members back into a shop

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, in the list, click the Shop you want to add a member to.
3. In the **Edit Shop** pane, click the **Access** tab.
4. On the **Access** tab, click **Excluded members**.

5. Select the check box next to the identity that you want to add to the shop as a member.
6. Click **Remove exclusion**.

Removing members from shops

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

NOTE: You can exclude members who have been added to the shop through a dynamic role. You can add these excluded members back to the shop later (see [Adding members to shops](#) on page 53). For more information about dynamic roles, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To remove a member from a shop

1. In the menu bar click **Setup > Shops**.
2. On the **Shops** page, click the shop in the list from which you want to remove a member.
3. In the **Edit Shop** pane, click the **Access** tab.
4. On the **Access** tab, select the check box next to the identity in the list that you want to remove as a member.
5. Click **Remove**.
6. If the member was assigned to the shop through a dynamic role, perform the following actions:
 - a. In the **Exclude members** pane, specify why you want to exclude the member.
 - b. Click **Exclude members**.

Managing requestable products in shops

You can decide which products can be requested from shops. Once products have been allocated to shelves in a shop (see [Making system entitlements requestable](#) on page 396) and labeled as requestable, they can be requested in the Web Portal by members of the shop.

Detailed information about this topic

- [Displaying requestable products](#) on page 54
- [Adding products to shelves](#) on page 55
- [Removing products from shelves](#) on page 55

Displaying requestable products

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

To display a shelf's requestable products

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

Adding products to shelves

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

To add a product to a shelf

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

Removing products from shelves

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

To remove a product from a shelf

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

6. On the **Products** tab, select the check box next to the product that you want to remove from the shelf.
7. Click **Remove**.

Deleting shops

You can delete shops.

NOTE: Before you can delete a shop, you must delete all shelves from the shop (see [Deleting shop shelves](#) on page 52) and remove all members from the shop (see [Removing members from shops](#) on page 54).

To delete a shop

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

Managing service categories

Use the Web Portal to display and edit service categories.

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

You can assign the product's service items to these service categories (see [Editing system entitlement service items](#) on page 404).

Detailed information about this topic

- [Displaying service categories](#) on page 56
- [Creating service categories](#) on page 57
- [Editing service categories](#) on page 59
- [Deleting service categories](#) on page 61

Displaying service categories

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

To display service categories

1. In the menu bar, click **Setup > Service categories**.
This opens the **Service Categories** page and displays all the service categories.

2. (Optional) To display details of a service category, click the appropriate service category.

Creating service categories

You can create service categories.

To create a service category

1. On the menu bar, click **Setup > Service categories**.
2. On the **Service Categories** page, click **+ Create service category**.
3. In the **Create Service Category** pane, enter the service category's main data.

You can edit the following main data.

Table 14: Service category main data

Property	Description
Service category	Enter a full, descriptive name for the service category.
Description	Enter a description for the service category.
Parent service category	To structure service categories hierarchically, click Select/Change and then select the parent service category.
Attestors	Click Select/Change and then select an application role. Members of this application role can approve attestation cases that affect the service category.
Product owners	Click Select/Change and then select an application role. Members of this application role can edit the service category's main data. They can also be used as approvers in approval processes when requests for service items assigned to this service category.
Approval policies	Select the approval policy used to determine the approver when the service item is requested in the Web Portal. NOTE: The approval policy specified for a service category is inherited by all associated service items and all child service categories where this is not specified.
Sort order	Enter the way you want the service category's service items to be sorted.
Picture	Add a picture of the service category. Users see this picture when they make a request. If you do not insert a picture here, the picture of the assigned service category is used. Perform the following actions to do this: <ol style="list-style-type: none">1. Click Add/Change.2. Select an image from your medium.
Application	To assign an application to a service category, select the application.
Service items	Specify the products can be requested through the service category. Perform the following actions as well: <ol style="list-style-type: none">1. Click Select/Change.2. Select the check box next to the service item you want to assign to the service category. TIP: To remove a service item, deselect the relevant check

Property	Description
	<p>box in front of the service item. To remove all service items, click Clear selection.</p> <p>3. Click Apply.</p>

4. Click **Save**.

Editing service categories

You can edit service items.

To edit a service category

1. On the menu bar, click **Setup > Service categories**.
2. On the **Service Categories** page, click the service category that you want to edit.
3. In the **Edit Service Category** pane, enter the service category's main data.

You can edit the following main data.

Table 15: Service category main data

Property	Description
Service category	Enter a full, descriptive name for the service category.
Description	Enter a description for the service category.
Parent service category	To structure service categories hierarchically, click Select/Change and then select the parent service category.
Attestors	Click Select/Change and then select an application role. Members of this application role can approve attestation cases that affect the service category.
Product owners	Click Select/Change and then select an application role. Members of this application role can edit the service category's main data. They can also be used as approvers in approval processes when requests for service items assigned to this service category.
Approval policies	Select the approval policy used to determine the approver when the service item is requested in the Web Portal. NOTE: The approval policy specified for a service category is inherited by all associated service items and all child service categories where this is not specified.
Sort order	Enter the way you want the service category's service items to be sorted.
Picture	Add a picture of the service category. Users see this picture when they make a request. If you do not insert a picture here, the picture of the assigned service category is used. Perform the following actions to do this: <ol style="list-style-type: none"> 1. Click Add/Change. 2. Select an image from your medium.
Application	To assign an application to a service category, select the application.
Service items	Specify the products can be requested through the service category. Perform the following actions as well: <ol style="list-style-type: none"> 1. Click Select/Change. 2. Select the check box next to the service item you want to assign to the service category. TIP: To remove a service item, deselect the relevant check

Property	Description
	<p>box in front of the service item. To remove all service items, click Clear selection.</p> <p>3. Click Apply.</p>

4. Click **Save**.

Deleting service categories

You can delete existing service categories.

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

- The service category is not predefined. Whether a service category is predefined, you can see from the description (see [Displaying service categories](#) on page 56).
- Service items are no longer assigned to the service category. To remove service items, edit the service category and remove the assigned service items (see [Editing service categories](#) on page 59).
- There are no longer child service categories under the service category. To assign child service categories under another service category or to remove them again, edit the corresponding child service category and remove or change the parent service category (see [Editing service categories](#) on page 59).

To delete a service category

1. On the menu bar, click **Setup > Service categories**.
2. On the **Service Categories** page, click the service category that you want to delete.
3. In the **Edit Service Category** pane, click **Delete service category**.
4. In the **Delete Service Category** dialog, confirm the prompt with **Yes**.

Managing service items

Use the Web Portal to display and edit service items.

In order to request company resources in the Web Portal, a service item must be assigned to them. Service items contain additional information about company resources (for example, article number, request properties, product manager or approver for requests).

Detailed information about this topic

- [Managing my system entitlements' service items](#) on page 281
- [Managing service items for system entitlements](#) on page 400

- [Displaying service items](#) on page 62
- [Editing service items](#) on page 62

Displaying service items

You can display all service items.

To display all service items

1. In the menu bar, click **Setup > Service items**.
This opens the **Service Items** page and displays all the service items.
2. (Optional) To display details of a service item, click the appropriate service item.

Editing service items

You can display all service items.

To edit a service item

1. In the menu bar, click **Setup > Service items**.
2. On the **Service Items** page, click the service item that you want to edit.
3. In the **Service Item** pane, edit the service item's main data.

You can edit the following main data.

Table 16: Service item main data

Property	Description
Service item	Enter a name for the service item.
Description	Enter a description of the service item.
Service category	You can group different service items into service categories. To do this, click /Select/Change and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 56.
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Approval by multi-factor authentication	Select this check box if approvals of requests for this service item require multi-factor authentication.

Property	Description
Max. days valid	<p>Specify how long an identity can keep the product until it is automatically unsubscribed again.</p> <p>An identity keeps their requested products on the shelf until they unsubscribe from them themselves. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. Products that are intended to have a limited shelf life need to be marked with a validity period.</p>
Website	<p>Specify the URL of a web page that contains more information about the product. Use the following format: https://www.example.com or http://www.example.com.</p> <p>This field allows you to link product descriptions in the internet or intranet to the service item.</p>
Sort order	Specify how the service category is sorted.
Request property	<p>Select the request property using the additional request parameters that are defined for a request. If you do not select any request properties, the request properties of the associated service category are used.</p> <p>Requests can be given additional information though product-specific request properties such as the specific details of a product, its size, or color. A request property gathers all additional features together that can be given when requesting a product.</p>
Functional area	<p>Click Select/Change and then select the functional area to which you want to assign the service item.</p> <p>You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by functional area. To do this, service items must be assigned to functional areas. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p>
Attestor	Click Select/Change and then select an application role. Members of this application role can approve attestation cases that affect the service item.
Terms of use	Select the terms of use that the product's requester must accept.
Reason type on request	Select which type of reason is required when the

Property	Description
	<p>service item is requested.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on approval	<p>Select which type of reason is required when the service item request is approved.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on denial	<p>Select which type of reason is required when the service item request is denied.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Picture	<p>Enter a picture for the service item. Users see this picture when they make a request.</p> <p>Perform the following actions as well:</p> <ol style="list-style-type: none"> 1. Click Add/Change. 2. Select an image from your medium.
Hide in service catalog	<p>Set this check box if the service item is meant to be requestable but is not displayed in the service catalog.</p>
Request parameters must be defined per recipient	<p>Select the check box to enter additional request properties separately for each recipient of the associated product, if the product is requested for several recipients in one request procedure.</p>
Retain service item assignment on relocation	<p>Select the check box if you want requests for this service item to be retained when a customer or the</p>

Property	Description
	<p>product is moved.</p> <p>If an identity requests a product from a shop and changes the shop at a later date, a decision must be made about how to proceed with the existing request. The same applies if a product is moved to another shelf.</p>
Tags	Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.
Not requestable/Requestable	<p>Set the switch to Requestable if you want to request the product via the Web Portal.</p> <p>Set the switch to Not requestable if you do not want to request the product via the Web Portal.</p>
Product owner	<p>Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item.</p> <p>Specify which identities are responsible for the service item.</p> <ul style="list-style-type: none"> To specify members of a specific application role as product owners, perform the following actions: <ol style="list-style-type: none"> Under Product owner, enable the Select from roles option. In the Product owner field, click Select/Change. In the Edit Property pane, click the appropriate application role. To specify a specific identity as the product owner, perform the following actions: <ol style="list-style-type: none"> Under Product owner, enable the Select from identities option. In the Identity list, select the corresponding identity.

4. Click **Save**.

Managing product bundles

Product bundles help simplify the request process. For example, a product bundle may contain all the products a new identity needs to get started. If users use a product bundle to

make a request, you are not obliged to request all the products in the product bundle. If this is the case, users can select only those products they want from the product bundle.

Related topics

- [Requesting using product bundles](#) on page 82

Detailed information about this topic

- [Displaying product bundles](#) on page 66
- [Displaying products in product bundles](#) on page 66
- [Creating product bundles](#) on page 67
- [Sharing product bundles](#) on page 70
- [Stop sharing product bundles](#) on page 70
- [Editing product bundles](#) on page 68
- [Adding products to product bundles](#) on page 69
- [Removing products from product bundles](#) on page 69
- [Deleting product bundles](#) on page 71

Displaying product bundles

To obtain an overview of all the product bundles, you can display them and their associated content.

To display product bundles

1. In the menu bar, click **Requests > Product bundles**.
This opens the **Product Bundles** page.
2. (Optional) To display the details of a product bundle, click the product bundle.

Related topics

- [Requesting using product bundles](#) on page 82

Detailed information about this topic

- [Displaying products in product bundles](#) on page 66

Displaying products in product bundles

To obtain an overview of all the products contained in a product bundle, you can display them.

To display products in a product bundle

1. In the menu bar, click **Requests > Product bundles**.
2. On the **Product Bundles** page, click the product bundle with the products you want to display.
3. In the **Edit Request Template** pane, click the **Products** tab.
4. (Optional) To display the details of a product, click the respective product.

Related topics

- [Requesting using product bundles](#) on page 82

Creating product bundles

You can create product bundles on the **Product Bundles** page or via the [shopping cart](#).

To create a product bundle

1. In the menu bar, click **Requests > Product bundles**.
2. On the **Product Bundles** page, click **+ Create product bundle**.
3. In the **Create Product Bundle** pane, enter the product bundle's main data.
You can edit the following main data.

Table 17: Product bundle main data

Property	Description
Product bundle	Enter a meaningful name for the product bundle.
Description	Enter a description for the product bundle.

4. Click **Create**.

To create a product bundle from the shopping cart

1. In the menu bar, click **Requests > Shopping cart**.
NOTE: The list of products and options for handling them is only shown when there are products in the shopping cart (see [Adding products to the shopping cart](#) on page 72).
2. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you want to add to the product bundle.
3. Click **⋮ (Actions) > Create product bundle**.
4. In the **Create Product Bundle** pane, enter the product bundle's main data.

You can edit the following main data.

Table 18: Product bundle main data

Property	Description
Product bundle	Enter a meaningful name for the product bundle.
Description	Enter a description for the product bundle.

5. Click **Create**.

Related topics

- [Requesting using product bundles](#) on page 82

Editing product bundles

You can edit the details of your product bundles. You can also add more products to and remove products from product bundles that you created yourself (see [Adding products to product bundles](#) on page 69 and [Removing products from product bundles](#) on page 69).

To edit a product bundle

1. In the menu bar, click **Requests > Product bundles**.
2. On the **Product Bundles** page, click the product bundle that you want to edit.
| **NOTE:** You can only edit product bundles that you created yourself.
3. In the **Create Product Bundle** pane, edit the product bundle's main data.

You can edit the following main data.

Table 19: Product bundle main data

Property	Description
Product bundle	Enter a meaningful name for the product bundle.
Description	Enter a description for the product bundle.

| **TIP:** You can also share product bundles with other users here (see [Sharing product bundles](#) on page 70).

4. Click **Save**.

Detailed information about this topic

- [Adding products to product bundles](#) on page 69
- [Removing products from product bundles](#) on page 69

Adding products to product bundles

You can add more products to your existing requests templates.

To add a product to a product bundle

1. In the menu bar, click **Requests > Product bundles**.
2. On the **Product Bundles** page, click the product bundle to which you want to add a product.
| NOTE: You can only edit product bundles that you created yourself.
3. Click the **Products** tab.
4. On the **Products** tab, click **Add products**.
5. In the **Add Products to Product Bundle** pane, perform one of the following actions:
 - To see which products are available to you, enable the **Show my products** option.
 - To see which products are available to other identities, enable the **Show products of another identity** and, in the **Identity** menu, select the respective identity.
6. To select the appropriate products and add them to the product bundle, perform one of the following actions:
 - In the tile view (☰)
 - Add a product: In the tile of the product, click **Add**.
 - Add multiple products: Click on the tiles with the products and then, below the tiles, click **Add**.
 - In the list view (☰)
 - Add a product: Next to the product, click **Add**.
 - Add multiple products: Next to the products, select the check box and then, below the list, click **Add**.

Related topics

- [Requesting using product bundles](#) on page 82

Removing products from product bundles

You can remove products from your product bundles.

To remove a product from a product bundle

1. In the menu bar, click **Requests > Product bundles**.
2. On the **Product Bundles** page, click the product bundle with the product you want to remove.
| **NOTE:** You can only edit product bundles that you created yourself.
3. In the **Edit Product Bundle** pane, click the **Products** tab.
4. On the **Products** tab, select the check box next to the product that you want to remove.
5. Click  **Remove**.

Related topics

- [Requesting using product bundles](#) on page 82

Sharing product bundles

To allow other users to use your product bundles, you can share your private product bundles with other users.

To share a product bundle with other users

1. In the menu bar, click **Requests > Product bundles**.
2. On the **Product Bundles** page, select the check box next to the product bundle you want to share with other users.
3. Click **Share**.
Your private product bundle is becomes a public product bundle that other users can use.

Related topics

- [Requesting using product bundles](#) on page 82

Stop sharing product bundles

If you do not want to share product bundles with other users anymore, you can stop sharing them.

To stop sharing a product bundle with other users

1. In the menu bar, click **Requests > Product bundles**.
2. On the **Product Bundles** page, select the check box next to the product bundle you want to stop sharing.

3. Click **Unshare**.

The public product bundle becomes a private product bundle that only you can use.

Related topics

- [Requesting using product bundles](#) on page 82

Deleting product bundles

You can delete product bundles at any time.

| **NOTE:** You can only delete your own personal product bundles.

To delete a product bundle

1. In the menu bar, click **Requests > Product bundles**.
2. On the **Product Bundles** page, select the check box next to the product bundle you want to delete.
3. Click **Delete**.
4. In the **Delete Product Bundles** dialog, confirm the prompt with **Yes**.

Related topics

- [Requesting using product bundles](#) on page 82

Requesting products

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

You can complete a request in three steps:

1. Add the desired product to your shopping cart (see [Adding products to the shopping cart](#) on page 72).
2. Verify the shopping cart and amend the product requests as required (see [Managing products in the shopping cart](#) on page 73).
3. Submit the request (see [Submitting requests](#) on page 78).

Detailed information about this topic

- [Adding products to the shopping cart](#) on page 72
- [Managing products in the shopping cart](#) on page 73

- [Submitting requests](#) on page 78
- [Requesting products on the Saved for Later list](#) on page 89
- [Displaying and requesting other identity's products](#) on page 80
- [Requesting for other identities or subidentities](#) on page 79
- [Requesting privileged access](#) on page 82
- [Requests for Active Directory groups](#) on page 84

Adding products to the shopping cart

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

To add products to the shopping cart

1. In the menu bar, click **Requests > New request**.

This opens the **New Request** page and displays all the available products.

2. (Optional) To filter which products are displayed, perform one of the following actions:
 - In the search field, enter the name of a product you want to look for.
 - In the **Service Categories** pane, click on the service category whose products you want to display.

The relevant products are displayed.

TIP: If you want to change the selected service category, in the **Service Categories** pane, click on another service category or **Root category (all products)**.

If the service category contains subcategories, click **▸ (expand)** next to the corresponding service category.

To display the products of the main categories and subcategories combined, enable **Show products from child categories**.

3. Select the check box next to the product you want to request.

TIP: To select all the products displayed, select the first check box in the list.

To remove all products from the selection, click **✕ Deselect all**.

4. Click **Move to shopping cart**.

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

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

The products are added to the shopping cart. Now, you can check the request and, if necessary, add to each product request (see [Managing products in the shopping cart](#) on page 73). Then send the request (see [Submitting requests](#) on page 78).

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

Related topics

- [Managing products in the shopping cart](#) on page 73
- [Submitting requests](#) on page 78

Managing products in the shopping cart

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 72), you can delete individual product requests from the cart, add more details to them, or perform other actions.

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

To manage products in the shopping cart

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, edit the shopping cart.
You can perform the following actions:
 - Remove products from the shopping cart (see [Removing products from the shopping cart](#) on page 74)
 - Define the validity of the products (see [Setting the validity period of products in your shopping cart](#) on page 75)
 - Change the priority of the requests (see [Specifying the priority of products in your shopping cart](#) on page 76)
 - Enter reasons for the requests (see [Giving reasons for requests](#) on page 76)
 - Check the shopping cart for invalid products and remove them (see [Checking the shopping cart](#) on page 77)
 - Request products for multiple identities (see [Requesting products in the shopping cart for multiple identities](#) on page 77)
 - Place products on the Saved for Later list (see [Saving products for later](#) on page 88)
 - Show the Saved for Later list (see [Displaying Saved for Later list](#) on page 89)
3. Ensure you only have requests that you really want to submit in your cart.
Now you can send your request (see [Submitting requests](#) on page 78).

Related topics

- [Adding products to the shopping cart](#) on page 72
- [Submitting requests](#) on page 78
- [Managing the Saved for Later list](#) on page 88

Displaying the shopping cart

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 72), you can view all the products in your shopping cart along with their details.

To display the products in your shopping cart

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

Related topics

- [Adding products to the shopping cart](#) on page 72
- [Submitting requests](#) on page 78

Removing products from the shopping cart

After adding added products to your shopping cart (see [Adding products to the shopping cart](#) on page 72), you can remove them again.

To remove products from the shopping cart

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

To remove multiple products from the shopping cart

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you do not want to request anymore.

3. Click **⋮ (Actions) > Remove selected**.
4. In the **Remove Selected Products From Cart** dialog, confirm the prompt with **Yes**.

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

To remove all products from the shopping cart

- Delete the shopping cart. For more information, see [Deleting shopping carts](#) on page 78.

Related topics

- [Adding products to the shopping cart](#) on page 72
- [Submitting requests](#) on page 78

Setting the validity period of products in your shopping cart

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 72), you can set their validity period. Once a product's validity period has expired, it can no longer be used.

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

TIP: You can renew the validity of a currently assigned product. For more information, see [Renewing products with limit validity periods](#) on page 107.

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

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

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

Related topics

- [Adding products to the shopping cart](#) on page 72
- [Submitting requests](#) on page 78

Specifying the priority of products in your shopping cart

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 72), you can specify their priority. The priority allows approvers to quickly identify how important a product request is.

To specify the priority of a product in the shopping cart

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

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

Related topics

- [Adding products to the shopping cart](#) on page 72
- [Submitting requests](#) on page 78

Giving reasons for requests

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 72), you can give reasons for requesting them. A reason can help approvers make their approval decisions.

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

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

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

Related topics

- [Adding products to the shopping cart](#) on page 72
- [Submitting requests](#) on page 78

Checking the shopping cart

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

To check your shopping cart for invalid products

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

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

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

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

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

Related topics

- [Adding products to the shopping cart](#) on page 72
- [Submitting requests](#) on page 78

Requesting products in the shopping cart for multiple identities

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 72), you can request the products in your shopping cart for other identities as well.

To request a product in the shopping cart for multiple identities

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

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

Related topics

- [Requesting for other identities or subidentities](#) on page 79
- [Adding products to the shopping cart](#) on page 72
- [Submitting requests](#) on page 78

Deleting shopping carts

You can clear your shopping cart at any time.

To delete your shopping cart

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

Related topics

- [Removing products from the shopping cart](#) on page 74
- [Adding products to the shopping cart](#) on page 72

Submitting requests

After you have added products to your shopping cart (see [Adding products to the shopping cart](#) on page 72), and edited and, if necessary, checked the request (see [Managing products in the shopping cart](#) on page 73), you can submit your shopping cart.

To submit your requests

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

This checks, submits, and triggers the request workflow.

TIP: To check the request's validity before you submit the request, click **⋮ (Actions) > Check shopping cart**. You can solve most problems of invalid product requests in the shopping cart by removing the problem product from the shopping cart (see [Checking the shopping cart](#) on page 77 and [Removing products from the shopping cart](#) on page 74).

Related topics

- [Adding products to the shopping cart](#) on page 72
- [Managing products in the shopping cart](#) on page 73
- [Checking the shopping cart](#) on page 77
- [Removing products from the shopping cart](#) on page 74

Requesting for other identities or subidentities

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

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

TIP: You can also request products for other identities directly from the shopping cart. For more information, see [Requesting products in the shopping cart for multiple identities](#) on page 77.

To request products for another identity

1. In the menu bar, click **Requests > New request**.
2. Click the **Recipient** field.
3. In the **Edit Recipient** pane, in the list, select the check boxes next to the identities you want to request products for.
TIP: To remove an identity from the recipient list, clear the check box next to the identity.
4. Click **Apply**.
5. Add the products that you want to request for the selected identity to the shopping cart (see [Adding products to the shopping cart](#) on page 72).
6. (Optional) Edit the shopping cart (see [Managing products in the shopping cart](#) on page 73).
7. Submit the request (see [Submitting requests](#) on page 78).

Related topics

- [Requesting products in the shopping cart for multiple identities](#) on page 77

Displaying and requesting other identity's products

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

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

Related topics

- [Requesting products in the shopping cart for multiple identities](#) on page 77
- [Requesting for other identities or subidentities](#) on page 79

Detailed information about this topic

- [Requesting products through reference users](#) on page 80
- [Requesting products through peer groups](#) on page 81

Requesting products through reference users

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

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

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, click the **Products by Reference User** tab.
3. In the **Select Reference User** pane, select the identity whose products you also want to request.

The **Products** and **Organizational units** tabs list requests, memberships, and entitlements of the selected identity.

4. Add the products that you want to save for later, to the shopping cart (see [Adding products to the shopping cart](#) on page 72).
5. Click **Go to cart**.
6. On the **My Shopping Cart** page, click **Submit**.

TIP: You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 73.

Related topics

- [Requesting products through peer groups](#) on page 81
- [Managing products in the shopping cart](#) on page 73

Requesting products through peer groups

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

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

To request other identities' products

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, click the **Recommended Products** tab.
The **Products** and **Organizational units** tabs list requests, memberships, and entitlements of the selected identity's peer group.
3. (Optional) If you want to make a request for another identity or check which products have been requested by their peer group, proceed as follows:
 - a. Click the **Recipient** field.
 - b. In the **Select Recipients** pane, click **Clear selection** and, in the list, select the check box next to the identity for which you want to request products.
NOTE: The list may contain a maximum of one identity. To remove an identity from the list, clear the check box next to the respective identity.
 - c. Click **Apply**.
4. Add the products that you want to save for later, to the shopping cart (see [Adding products to the shopping cart](#) on page 72).
5. Click **Go to cart**.
6. On the **My Shopping Cart** page, click **Submit**.

TIP: You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 73.

Related topics

- [Requesting products through reference users](#) on page 80
- [Managing products in the shopping cart](#) on page 73

Requesting using product bundles

You can use your own (private) product bundles or product bundles that are shared with all users (public) for making requests. Product bundles help simplify the request process. For example, a product bundle may contain all the products a new identity needs to get started. If you use a product bundle to make a request, you are not obliged to request all the products in the product bundle. You only have to select the products you want from it.

TIP: To find out how you can request the same products as another identity, see [Requesting products through reference users](#) on page 80.

To request products using a product bundle

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, click the **Product Bundles** tab.
3. In the **Product bundles** section, click the product bundle whose products you want to request.

TIP: To display more information about the product bundle, click **Info** next to the product bundle name.

4. Perform one of the following tasks:
 - Request individual products from the product bundle: Select the check box next to the product you want to request.
 - Request all products from the product bundle: Click **Select product bundle**.
5. Click **Move to shopping cart**.
6. Click **Go to cart**.
7. On the **Shopping Cart** page, click **Submit**.

TIP: You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 73.

Related topics

- [Managing product bundles](#) on page 65
- [Managing products in the shopping cart](#) on page 73
- [Requesting products through reference users](#) on page 80

Requesting privileged access

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

TIP: For more information on the topic of Privileged Account Management, see the *One Identity Manager Administration Guide for Privileged Account Governance*.

To request privileged access

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, in the **Service Categories** pane, click the **Privileged Access Requests** service category.
3. Select how you want to access the system by selecting the check box in front of the corresponding option:
 - **Password release request:** Request a temporary password.
 - **Remote desktop session request:** Request temporary access through a remote desktop connection.
 - **SSH key request:** Request temporarily valid SSH key.
 - **SSH session request:** Request temporary access through an SSH session.
 - **Telnet session requests:** Request temporary access using a Telnet session.
4. Click **Add to cart**.
5. In the **Request Details** pane, expand the selected product.
6. In the **PAM user account** menu, select the PAM user account that you want to use for PAM access.
7. Depending on the type of access you have selected, perform one of the following actions:
 - Password request or SSH key request:
 1. In the **System to access** field, click **Select**.
 2. In the **Edit Property** pane, select whether you want to request access for a **PAM asset** or a **PAM directory**.
 3. Next to the corresponding PAM directory or PAM asset, click **Select**.
 - Remote desktop session request, SSH session request, or Telnet session request: In the **System to access**, select the corresponding PAM asset.
8. Perform the following actions:
 - a. In the **Account to access** field, click **Select**.
 - b. In the **Edit Property** pane, select whether you want to request access for a **PAM asset account** or a **PAM directory account**.
 - c. Next to the corresponding PAM asset account or PAM directory account, click **Select**.
9. (Optional) In the **Comment** field, enter a comment, for example, to justify why you are requesting this access.
10. In the **Valid from** field, specify the time from which you want the access to be valid or clear the check box so that access is valid from the time of this request.
11. 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. For example, if you have specified that the access is valid from 12 noon tomorrow and should be valid for 60 minutes, then the validity period will expire at 1 pm tomorrow.

12. Click **Apply**.
13. (Optional) Repeat the steps for all other users and access types.
14. Click **Submit**.
15. Click **Go to cart**.
16. On the **Shopping Cart** page, click **Submit**.

TIP: You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 73.

Once the request has been approved, a button will appear in the request details pane of the request history (see [Displaying request history](#) on page 105) that you can use to log in to the Privileged Account Management system to obtain the login credentials.

Related topics

- [Managing products in the shopping cart](#) on page 73

Requests for Active Directory groups

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

Detailed information about this topic

- [Requesting new Active Directory groups](#) on page 84
- [Requesting changes to Active Directory groups](#) on page 85
- [Requesting deletion of Active Directory groups](#) on page 86

Requesting new Active Directory groups

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

To request a new Active Directory group

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, in the **Service Categories** pane, click the **Active Directory groups** service category.

3. Perform one of the following actions:
 - To request a new Active Directory security group, select the check box next to **New Active Directory security group**.
 - To request a new Active Directory distribution group, select the check box next to **New Active Directory distribution group**.
4. Click **Add to cart**.
5. In the **Request Details** pane, perform one of the following actions:
 - As a requester without responsibility for the target system, enter a name for the new group in the **Suggested name** field.
 - As the target system manager, provide additional details about the new group:
 - **Name:** Enter a name for the group.
 - **Group scope:** Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can select one of the following group scopes:
 - **Global group:** Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group's domain.
 - **Local:** Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.
 - **Universal:** Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
 - **Container:** Click **Select** and select a container for the group.
6. Click **Apply**.
7. Click **Submit**.

TIP: You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 73.
8. Click **Go to cart**.
9. On the **Shopping Cart** page, click **Submit**.

Related topics

- [Approving pending requests from newly created Active Directory groups](#) on page 94

Requesting changes to Active Directory groups

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

To change an Active Directory group

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

TIP: You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 73.
10. Click **Go to cart**.
11. On the **Shopping Cart** page, click **Submit**.

Requesting deletion of Active Directory groups

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

To delete an Active Directory group

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, in the **Service Categories** pane, click the **Active Directory groups** service category.

3. Select the check box next to **Delete Active Directory group**.
 4. Click **Add to cart**.
 5. In the **Request Details** pane, in the **Active Directory group to delete** menu, select the Active Directory group that you want to delete.
 6. Click **Apply**.
 7. Click **Submit**.
- TIP:** You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 73.
8. Click **Go to cart**.
 9. On the **Shopping Cart** page, click **Submit**.

Requesting new SharePoint groups

To create a new SharePoint group, you must request the **New SharePoint Group** product.

To request a new SharePoint group

1. In the menu bar, click **Requests > New request**.
2. On the **New Request** page, in the **Service Categories** pane, click the **SharePoint groups** service category.
3. Select the check box next to **New SharePoint group**.
4. Click **Add to cart**.
5. In the **Request Details** pane, perform one of the following actions:
 - As a requester without responsibility for the target system, enter a name for the new group in the **Suggested name** field.
 - As the target system manager, provide additional details about the new group:
 - **Site collection:** Select a site collection where the group will be applied. A site collection groups sites together. User account and their access permissions are managed on the sites.
 - **Display name:** Enter a name for the new group.
 - **Description:** Enter a description for the SharePoint group.
6. Click **Apply**.
7. Click **Submit**.

TIP: You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 73.

8. Click **Go to cart**.
9. On the **Shopping Cart** page, click **Submit**.

Related topics

- [Approving pending requests from newly created SharePoint groups](#) on page 96

Managing the Saved for Later list

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

Detailed information about this topic

- [Saving products for later](#) on page 88
- [Displaying Saved for Later list](#) on page 89
- [Requesting products on the Saved for Later list](#) on page 89
- [Removing products from the Saved for Later list](#) on page 90
- [Deleting the Saved for Later list](#) on page 91

Saving products for later

If you do not want to request products immediately but at a later date, you can save the products on the Saved for Later list. You can access your Saved for Later list at any time, move products from it into your shopping cart, and request them (see [Requesting products on the Saved for Later list](#) on page 89).

To add products to your Saved for Later list.

1. Add the products that you want to save for later, to the shopping cart (see [Adding products to the shopping cart](#) on page 72).
2. In the menu bar, click **Requests > Shopping cart**.
3. On the **Shopping Cart** page, in the list, select the check boxes next to the products that you want to save for later.
4. Click **⋮ (Actions) > Move to Saved for Later list**.

The products are moved with all their settings to your Saved for Later list.

Related topics

- [Managing products in the shopping cart](#) on page 73

Displaying Saved for Later list

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

To display your Saved for Later list

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

Related topics

- [Managing products in the shopping cart](#) on page 73

Requesting products on the Saved for Later list

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

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

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

TIP: You can also add more products to your shopping cart and configure various settings. For more information, see [Managing products in the shopping cart](#) on page 73.

Related topics

- [Managing products in the shopping cart](#) on page 73
- [Submitting requests](#) on page 78

Removing products from the Saved for Later list

You can remove products from your Saved for Later list. To delete the entire Saved for Later list, see [Deleting the Saved for Later list](#) on page 91.

To remove a product from your Saved for Later list

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

To remove multiple products from your Saved for Later list

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

Related topics

- [Managing products in the shopping cart](#) on page 73

Deleting the Saved for Later list

You can delete your Saved for Later list. For more information about removing individual products, see [Removing products from the Saved for Later list](#) on page 90.

To delete your Saved for Later list

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

Related topics

- [Managing products in the shopping cart](#) on page 73

Pending requests

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

Detailed information about this topic

- [Displaying pending requests](#) on page 91
- [Approving and denying requests](#) on page 93
- [Appointing other approvers for pending requests](#) on page 97
- [Rejecting request approval](#) on page 102
- [Managing inquiries about pending requests](#) on page 103

Displaying pending requests

If you are the approver of certain products and identities request these products, you can [display](#) the requests. Then you can make approval decisions about the pending requests (see [Approving and denying requests](#) on page 93).

You can also [display](#) request that you have placed that still need to be granted or denied approval by others.

To display pending requests

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

To display your pending requests so that others can grant or deny approval.

1. Open the home page.
2. On the home page, click **EXPLORE** in the **My Pending Requests** tile.
This opens the **Request History** page and display requests that you have made but still need to be granted or denied approval by someone else (see [Displaying request history](#) on page 105).

Detailed information about this topic

- [Displaying pending request history](#) on page 92
- [Displaying pending request entitlements](#) on page 92
- [Displaying rule violations of pending requests](#) on page 93

Displaying pending request history

You can display the history of request to get an overview of all the actions and approvals in a request's workflow.

To display an the history of a pending request

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click the request whose history you want to display.
3. In the **View Request Details** pane, click the **Workflow** tab.

Displaying pending request entitlements

You can display which entitlements are assigned to request recipients if the requests are granted approval.

To display entitlements of a pending request

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click the request whose entitlements you want to display.
3. In the **View Request Details** pane, click the **Entitlements** tab.

Displaying rule violations of pending requests

You can view which rule violations can be caused by requests if they are granted approval.

To display the rule violations of a pending request

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click the request whose rule violations you want to display.
3. In the **View Request Details** pane, click the **Rule Violations** tab.

Approving and denying requests

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

To make an approval decision about a pending request

1. In the menu bar, click **Requests > Pending requests**.
2. (Optional) To approve a request as a member of the chief approval team and only display the relevant requests, on the **Pending Requests** page, select the **Show requests to be approved by chief approval team** check box.
3. On the **Pending Requests** page, perform one of the following actions:
 - To approve a request, click **✓ Approve** next to the request.
 - To deny a request, click **⊘ Deny** next to the request.

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

4. On the **Approve Request/Deny Request** page, perform the following actions:
 - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
 - b. In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

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

Detailed information about this topic

- [Decision guidance for request approvals](#) on page 94
- [Approving pending requests from newly created Active Directory groups](#) on page 94
- [Approving pending requests from newly created SharePoint groups](#) on page 96
- [Approving new managers' pending requests](#) on page 96

Decision guidance for request approvals

To help you evaluate and approve pending requests, you can use decision guidance to view past request approvals in the current context.

To display decision guidance

1. In the menu bar, click **Requests > Pending requests**.
2. (Optional) To approve a request as a member of the chief approval team and only display the relevant requests, on the **Pending Requests** page, select the **Show requests to be approved by chief approval team** check box.
3. On the **Pending Requests** page, perform one of the following actions:
 - To approve a request, click **✓ Approve** next to the request.
 - To deny a request, click **⊗ Deny** next to the request.
4. In the **Approve Request/Deny Request** pane, click the **Decision Guidance** pane.
5. (Optional) To control which requests are displayed, on the **Decision Guidance** tab, click **▼ (Filter)** (see [Filtering](#) on page 27). For example, this allows you to show only requests for the same recipient.
6. (Optional) To display details of a request, click the appropriate request.

Approving pending requests from newly created Active Directory groups

Identities can create Active Directory groups by requesting the **New Active Directory security group** or the **New Active Directory distribution group** product. As approver,

you can make approval decisions about requests like this. If you approve the request, you must provide additional information about the group.

To approve a request to create a new Active Directory group

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click ✓ **Approve** next to the request for a new Active Directory group.
3. In the **Approve Request** section, enter additional information about the new group:
 - **Name:** Enter a name for the group.
 - **Group scope:** Select the scope that specifies the range of the group's usage within the domain or forest. The group's scope specifies where the group is allowed to issue permissions. You can select one of the following group scopes:
 - **Global group:** Global groups can be used to provide cross-domain authorizations. Members of a global group are only user accounts, computers, and groups belonging to the global group's domain.
 - **Local:** Local groups are used when authorizations are issued within the same domain. Members of a domain local group can be user accounts, computers, or groups in any domain.
 - **Universal:** Universal groups can be used to provide cross-domain authorizations available. Universal group members can be user accounts and groups from all domains in one domain structure.
 - **Container:** Click **Select/Change** and select a container for the group.
4. (Optional) To specify a validity period for the Active Directory group, perform the following actions:
 - a. In the **Valid from** field, specify as from when the Active Directory groups are valid.
 - b. In the **Valid until** field, specify until when the Active Directory groups are valid.
5. Perform the following actions:
 - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
 - b. In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

NOTE: For more detailed information about standard reasons, see the [One Identity Manager IT Shop Administration Guide](#).
6. Click **Save**.

Related topics

- [Requesting new Active Directory groups](#) on page 84

Approving pending requests from newly created SharePoint groups

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

To approve a request to create a new SharePoint group

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click ✓ **Approve** next to the request for a new SharePoint group.
3. In the **Approve Request** section, enter additional information about the new group:
 - **Site collection:** Select a site collection where the group will be applied. A site collection groups sites together. User account and their access permissions are managed on the sites.
 - **Display name:** Enter a name for the new group.
 - **Description:** Enter a description for the SharePoint group.
4. (Optional) To specify a validity period for the SharePoint group, perform the following actions:
 - a. In the **Valid from** field, specify as from when the SharePoint groups are valid.
 - b. In the **Valid until** field, specify until when the SharePoint groups are valid.
5. Perform the following actions:
 - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
 - b. In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

NOTE: For more detailed information about standard reasons, see the [One Identity Manager IT Shop Administration Guide](#).
6. Click **Save**.

Related topics

- [Requesting new SharePoint groups](#) on page 87

Approving new managers' pending requests

Managers can allocate new managers for their identities. To do this, they must select the new manager and a deadline in the future for changing managers (see [Assigning other](#)

[managers to my identities](#) on page 224). An assignment of this type triggers a request of type **New manager assignment**.

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

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

To approve an escalated assignment to a new manager

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, next to the **New manager assignment** request, click **✓ Approve**.
3. In the **Approve Request** page, expand the **New manager assignment** pane.
4. (Optional) If the identity has already been assigned entitlements or products, these will be removed or unsubscribed by default on the effective date. If you want the identity to retain these entitlements or products when transferring to the new manager, disable the check boxes next to the respective entitlements and products.
5. (Optional) To specify from when the new manager is responsible for the identity, enter the date in the **Valid from** field. If you leave the field blank, the change of manager will be carried out immediately after approval.
6. In the **Approve Request** pane, perform one of the following actions:
 - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
 - b. In the **Additional comments about your decision** field, enter extra information about your approval decision.
7. Click **Save**.

Related topics

- [Assigning other managers to my identities](#) on page 224

Appointing other approvers for pending requests

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

- **Reroute approval**
You give the task of approving to another approval level (see [Rerouting approvals of pending requests](#) on page 98).
- **Appoint additional approver**
You delegate the task of approving to another identity (see [Appointing additional](#)

[approvers to pending requests](#) on page 99). The additional approver must make an approval decision in addition to the other approvers.

The additional approver can reject the approval and return it to you (see [Rejecting request approval](#) on page 102).

You can withdraw an additional approver. For example, if the other approver is not available.

- **Delegate approval**

You delegate the task of approving to another approval level (see [Delegating approvals of pending requests to other identities](#) on page 100). This identity is added as approver in the current approval step and makes approval decisions on your behalf.

The new approver can reject the approval and return it to you (see [Rejecting request approval](#) on page 102).

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

Rerouting approvals of pending requests

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

To reroute an approval

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

To reroute multiple approvals

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

Appointing additional approvers to pending requests

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

To add an additional approver

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

To add an additional approver to multiple requests

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

Related topics

- [Removing additional approvers of pending requests](#) on page 99

Removing additional approvers of pending requests

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

To withdraw a request's additional approver

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

To withdraw additional approver from multiple requests

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

Related topics

- [Appointing additional approvers to pending requests](#) on page 99

Delegating approvals of pending requests to other identities

You can delegate an approval decision about a request to another identity. You can revoke this action in the approval history (see [Withdrawing delegations from pending requests](#) on page 101).

To delegate an approval

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

To delegate approval of multiple requests

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

Related topics

- [Withdrawing delegations from pending requests](#) on page 101

Withdrawing delegations from pending requests

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

To withdraw an approval delegation

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

To withdraw multiple delegations from approvals

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

Related topics

- [Delegating approvals of pending requests to other identities](#) on page 100

Escalating approvals of pending requests

You can escalate the approval of a product request. The request is presented to another approval body. The request is then further processed in the normal approval workflow.

To escalate approval for a request

1. In the menu bar, click **Request > My Actions**.
2. In the menu bar, click **Requests > Pending requests**.
3. On the **Pending Requests** page, in the list, select the check box next to the request whose approval you want to escalate.
4. Click **⋮ Actions > Escalate approval**.
5. In the **Escalate Approval** pane, in the **Reason for your decision** field, enter a reason for the escalation.
6. Click **Save**.

Rejecting request approval

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

To reject an approval

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

To reject approval of multiple requests

1. In the menu bar, click **Requests > Pending requests**.
 2. On the **Pending Requests** page, in the list, select the check boxes next to the requests that you do not want to make an approval decision about.
 3. Click **⋮ Actions > Reject approval**.
 4. In the **Reject Approval** pane, in the **Reason for your decision** pane, enter a reason for the rejecting.
 5. Click **Save**.
- [Appointing additional approvers to pending requests](#) on page 99

Managing inquiries about pending requests

To gather information about pending requests, you can send inquiries about them to any identity.

Once you have sent an inquiry about a request, the request is reserved for you (Hold status). As long as the request is reserved for you, only you or the chief approval team can make an approval decision about the request. You can withdraw the inquiry at any time. You can cancel the reservation at any time so that another approver can make an approval decision about the request.

Related topics

- [Managing request inquiries directed at you](#) on page 111
- [Managing inquiries about pending attestation cases](#) on page 145

Detailed information about this topic

- [Sending inquiries about pending requests](#) on page 103
- [Recalling inquiries about pending requests](#) on page 104
- [Canceling reservations of pending requests](#) on page 104
- [Displaying answers to inquiries about pending requests](#) on page 105

Sending inquiries about pending requests

Before you make an approval decision about a request, you can send a question to an identity about it.

NOTE: Once you have sent an inquiry about a request, the request is reserved for you (Hold status). As long as the request is reserved for you, only you or the chief approval team can make an approval decision about the request.

You can revoke the reservation with the following actions:

- Withdraw the inquiry (see [Recalling inquiries about pending requests](#) on page 104)
- Cancel the reservation (see [Canceling reservations of pending requests](#) on page 104)

To make an inquiry

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click the request that you want to inquire about.
3. In the **View Request Details** pane, click **Send inquiry**.
4. In the **Send Inquiry** pane, in the **Recipient of the inquiry** menu, select the identity to which you want to send the inquiry.

5. In the **Inquiry** field, enter your inquiry.
6. Click **Save**.

Related topics

- [Managing request inquiries directed at you](#) on page 111

Recalling inquiries about pending requests

If your issue with a request has become irrelevant, you can withdraw your inquiry. Once you have withdrawn the inquiry, the request reservation is also revoked and all the original approvers can approve the request again.

To withdraw and inquiry

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click the request that you inquired about.
3. In the **View Request Details** pane, click **Withdraw inquiry**.
4. (Optional) In the **Withdraw Inquiry** pane, in the **Reason for your decision** field, enter why you are withdrawing the inquiry.
5. Click **Save**.

Related topics

- [Managing request inquiries directed at you](#) on page 111

Canceling reservations of pending requests

Once you have sent an inquiry about a request, the request is reserved for you (Hold status). As long as the request is reserved for you, only you or the chief approval team can make an approval decision about the request.

To release the request again for approval and to allow other approvers to edit it, you can revoke the reservation with the following actions:

- You can withdraw the inquiry (see [Recalling inquiries about pending requests](#) on page 104).
- You can cancel the inquiry manually.

To cancel a reservation

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click the request that you inquired about.
3. In the **View Request Details** pane, click **Cancel reservation**.

4. (Optional) In the **Cancel Reservation** pane, in the **Reason for your decision**, enter a reason for canceling the reservation.
5. Click **Save**.

Related topics

- [Managing request inquiries directed at you](#) on page 111

Displaying answers to inquiries about pending requests

If the identity you sent an inquiry to has responded to it, you can view their answer in the workflow of the respective request.

To display an answer

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click the request that you inquired about.
3. In the **View Request Details** pane, click the **Workflow** tab.
In the workflow, the response is displayed under **Answer**.

Related topics

- [Managing request inquiries directed at you](#) on page 111

Displaying request history

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

To display the request history

1. In the menu bar, click **Requests > Request history**.
This opens the **Request History** page.
2. (Optional) To control which requests are displayed, click **▼ (Filter)** (see [Filtering](#) on page 27). For example, this allows you to show just pending requests (no approval decision yet made).
3. (Optional) To display details of a request, click the request whose details you want to see.

Related topics

- [Canceling requests](#) on page 106
- [Renewing products with limit validity periods](#) on page 107
- [Unsubscribing products](#) on page 108

Canceling requests

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

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

To cancel a request

1. In the menu bar, click **Requests > Request history**.
2. On the **Request History** page, click **▼ (Filter)**.
3. In the filter context menu, select the **Pending** check box.
4. (Optional) To control which requests are displayed, click **▼ (Filter)** (see [Filtering](#) on page 27). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to cancel a request of another identity, in the **🔍 Search** field, enter the identity's name.
6. Click the product with the request you want to cancel.
7. In the **View Request Details** pane, click **Cancel request**.
8. In the **Cancel request** pane, in the **Reason for your decision** field, enter a reason for the cancellation.
9. Click **Save**.

To cancel multiple requests

1. In the menu bar, click **Requests > Request history**.
2. On the **Request History** page, click **▼ (Filter)**.
3. In the filter context menu, select the **Pending** check box.
4. (Optional) To control which requests are displayed, click **▼ (Filter)** (see [Filtering](#) on page 27). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to cancel requests belonging to another identity, in the **🔍 Search** field, enter the identity's name.
6. Select the check boxes next to the requests you want to cancel.
7. Click **⋮ Actions > Cancel request**.

8. In the **Cancel request** pane, in the **Reason for your decision** field, enter a reason for the cancellation.
9. Click **Save**.

Related topics

- [Requesting products](#) on page 71
- [Displaying request history](#) on page 105
- [Renewing products with limit validity periods](#) on page 107
- [Unsubscribing products](#) on page 108

Renewing products with limit validity periods

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

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

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

To renew a product's validity period

1. In the menu bar, click **Requests > Request history**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, select the **Active** check box.
4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see [Filtering](#) on page 27). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to renew a product of another identity, in the 🔍 **Search** field, enter the identity's name.
6. Click the product that you want to renew.
7. In the **View Request Details** pane, click **Renew product**.
8. In the **Renew Product** pane, perform the following actions:
 - a. In the **Renewal date** field, enter the renewal date for the product. If the field is empty the product has unlimited availability.
 - b. In the **Reason for your decision** field, enter a reason for the renewal.
 - c. Click **Save**.

To renew the validity period of multiple products

1. In the menu bar, click **Requests > Request history**.
2. On the **Request History** page, click **▼ (Filter)**.
3. In the filter context menu, select the **Active** check box.
4. (Optional) To control which requests are displayed, click **▼ (Filter)** (see [Filtering](#) on page 27). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to renew products of another identity, in the **Search** field, enter the identity's name.
6. Select the check boxes next to the products you want to renew.
7. Click **⋮ Actions > Renew product**.
8. In the **Renew Product** pane, perform the following actions:
 - a. In the **Renewal date** field, enter the renewal date for the products. If the field is empty the products have unlimited availability.
 - b. In the **Reason for your decision** field, enter a reason for the renewal.
 - c. Click **Save**.

Related topics

- [Setting the validity period of products in your shopping cart](#) on page 75
- [Canceling requests](#) on page 106
- [Unsubscribing products](#) on page 108

Unsubscribing products

You can unsubscribe from products that are already assigned if they are no longer required. Products that can be unsubscribed have the **Assigned** status.

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

To unsubscribe a product

1. In the menu bar, click **Requests > Request history**.
2. On the **Request History** page, click **▼ (Filter)**.
3. In the filter context menu, select the **Active** check box.
4. (Optional) To control which requests are displayed, click **▼ (Filter)** (see [Filtering](#) on page 27). For example, this allows you to show just requests that you have carried out for other identities.

5. (Optional) If you want to unsubscribe a product of another identity, in the 🔍 **Search** field, enter the identity's name.
6. Click the product that you want to unsubscribe.
7. In the **View Request Details** pane, click **Unsubscribe product**.
8. In the **Unsubscribe Product** pane, perform the following actions:
 - a. In the **Unsubscribed as from** field, enter the date for unsubscribing the product. If you leave this field empty, the product is unsubscribed once you have clicked **Saved**.
 - b. In the **Reason for your decision** field, enter a reason for unsubscribing.
 - c. In the **Additional comments about your decision** field, enter extra information about unsubscribing.
 - d. Click **Save**.

To unsubscribe multiple products

1. In the menu bar, click **Requests > Request history**.
2. On the **Request History** page, click ▼ (**Filter**).
3. In the filter context menu, select the **Active** check box.
4. (Optional) To control which requests are displayed, click ▼ (**Filter**) (see [Filtering](#) on page 27). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to unsubscribe products of another identity, in the 🔍 **Search** field, enter the identity's name.
6. In the list, select the check boxes next to the products you want to unsubscribe.
7. Click **⋮ Actions > Unsubscribe product**.
8. In the **Unsubscribe Product** pane, perform the following actions:
 - a. In the **Unsubscribed as from** field, enter the date for unsubscribing the products. If you leave this field empty, the products are unsubscribed once you have clicked **Saved**.
 - b. In the **Reason for your decision** field, enter a reason for unsubscribing.
 - c. In the **Additional comments about your decision** field, enter extra information about unsubscribing.
 - d. Click **Save**.

Related topics

- [Displaying request history](#) on page 105
- [Renewing products with limit validity periods](#) on page 107
- [Canceling requests](#) on page 106

Displaying requests

You can display all the requests for which you have made approval decisions.

To display approvals

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

Related topics

- [Withdrawing delegations from pending requests on page 101](#)
- [Removing additional approvers of pending requests on page 99](#)
- [Approving and denying requests on page 93](#)
- [Undoing approvals on page 110](#)

Undoing approvals

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

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

To undo an approval

1. In the menu bar, click **Requests > Request history**.
2. (Optional) To control which requests are displayed on the **Request History** page, click ▼ (**Filter**) (see [Filtering](#) on page 27). For example, this allows you to show just pending requests (no approval decision yet made).
3. In the list, click the request whose approval you want to undo.
4. In the **View Request Details** pane, click **Undo approval decision**.
5. In the **Undo Approval Decision** dialog, perform the following actions:
 - a. In the **Reason for your decision** field, enter why you want to undo the approval.
 - b. Click **Save**.

Related topics

- [Displaying requests](#) on page 110

Managing request inquiries directed at you

To gather more information about a pending request, the approver can send you an inquiry about the request. After you have answered the inquiry, the approver can make their approval decision.

Related topics

- [Managing inquiries about pending requests](#) on page 103
- [Managing attestation inquiries directed at you](#) on page 149

Detailed information about this topic

- [Displaying request inquiries](#) on page 111
- [Answering inquiries about requests](#) on page 111

Displaying request inquiries

You can display inquiries about a product request that have been sent to you and to which you must respond.

To view inquiries directed at you

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click the **Inquiries** tab.
3. (Optional) To see more information about the answer to a request inquiry, click the respective inquiry.

Related topics

- [Managing inquiries about pending requests](#) on page 103

Answering inquiries about requests

You can respond to inquiries that have been made to you about a product request.

| **TIP:** If you respond to inquiries, do not grant or deny approval for the request.

To respond to inquiries

1. In the menu bar, click **Requests > Pending requests**.
2. On the **Pending Requests** page, click the **Inquiries** tab.
3. On the **Inquiries** tab, next to the inquiry you want to answer, click the **Reply to inquiry**.
4. In the **Answer Question** pane, enter your answer in the **Reply to inquiry** field.
5. Click **Save**.

Related topics

- [Sending inquiries about pending requests](#) on page 103

Attestation

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

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

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

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

Detailed information about this topic

- [Sending attestation reminders](#) on page 132
- [Pending attestations](#) on page 136
- [Displaying attestation history](#) on page 148
- [Managing attestation inquiries directed at you](#) on page 149
- [Managing attestations](#) on page 113

Managing attestations

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

verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Detailed information about this topic

- [Attestation policy settings](#) on page 114
- [Starting attestation](#) on page 124
- [Running sample attestations](#) on page 125
- [Managing attestation runs](#) on page 126
- [Attestation by peer group analysis](#) on page 129
- [Managing samples](#) on page 130

Attestation policy settings

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

Detailed information about this topic

- [Displaying attestation policies](#) on page 114
- [Setting up attestation policies](#) on page 116
- [Editing attestation policies](#) on page 118
- [Copying attestation policies](#) on page 121
- [Deleting attestation policies](#) on page 124
- [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431

Displaying attestation policies

To obtain an overview, you can display attestation policies.

To display attestation policies

1. In the menu bar, click **Attestation > Attestation Policies**.
This opens the **Attestation Policies** page.
2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click **✕ (Clear filter)** next to the filter.
3. (Optional) To display the attestation run of an attestation policy, click next to the attestation policy, **⋮ Actions > View attestation runs**.

Related topics

- [Displaying attestation policies main data](#) on page 115

Displaying attestation policies main data

To obtain an overview of attestation policy definitions and the objects that will be attested through them, you can display the attestation policy main data.

To display main data of an attestation policy

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

Displaying attestation policy reports

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

To display an attestation policy's report

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

Related topics

- [Displaying attestation run reports](#) on page 128

Setting up attestation policies

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

To create a new attestation policy

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

You can edit the following main data.

Table 20: Attestation policy main data

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

Property	Description
	you do not want to specify a time, enter 0 .
Owner	Select the identity that is responsible for this attestation policy. This identity can view and edit the attestation policy.
Risk index	Use the slider to define the attestation policy's risk index. This value specifies the risk for the company if attestation for this attestation policy is denied.
Compliance frameworks	Click Select/Change and select the relevant compliance frameworks for the attestation policy. Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements.
Policy collection	Select the policy collection to which you want to assign the attestation policy. To start attesting several attestation policies at the same time, you can group different attestation policies into a so-called policy collection (see Grouping attestation policies (using policy collections) on page 132).
Sample	Select which sampling data to use (see Running sample attestations on page 125 and Managing samples on page 130). NOTE: You can only select samples that have not yet been assigned to an attestation policy. NOTE: When you select samples, you can not set conditions anymore and vice versa.
Close obsolete tasks automatically	Specify whether attestation cases pending for this attestation policy are automatically closed if new attestation cases are created (for example, when there is a new attestation run of this attestation policy). If an attestation run with this attestation policy is started and the option is set, new attestation cases are created according to the condition. All pending, obsolete attestation cases for newly determined attestation objects of this attestation policy are stopped. Attestation cases for attestation objects that are not recalculated, remain intact.
Approval by multi-factor authentication	Specify whether approvals about attestation cases governed by this attestation policy require multifactor authentication.

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

5. In the **Condition type** menu, click the condition type to use (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431).

NOTE: The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.

6. (Optional) Depending on which condition type you have selected, you can filter the selection of objects to attest (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431).
7. (Optional) Create more conditions if required. To do this, click **Add another condition**.
8. (Optional) If you have specified more than one condition, you must specify whether one or all of the conditions must be fulfilled by enabling the appropriate option:
 - **All conditions must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects fulfilling all of the conditions. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.
 - **At least one condition must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects that fulfill at least one of the conditions. Use of this option generates a superset of all the individual conditions of the selected objects.
9. Click **Create**.

Related topics

- [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431

Editing attestation policies

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

To edit an attestation policy

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

TIP: To show disabled attestation policies, delete the **Activated attestation policies** option. To do this, click  next to the filter (**Clear filter**).

NOTE: The system contains default attestation policies. These policies can only be edited to a limited degree. If you want to make changes to a default attestation policy, create a copy and edit the copy (see [Copying attestation policies](#) on page 121).

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

You can edit the following main data.

Table 21: Attestation policy main data

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

Property	Description
	Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements.
Policy collection	<p>Select the policy collection to which you want to assign the attestation policy.</p> <p>To start attesting several attestation policies at the same time, you can group different attestation policies into a so-called policy collection (see Grouping attestation policies (using policy collections) on page 132).</p>
Sample	<p>Select which sampling data to use (see Running sample attestations on page 125 and Managing samples on page 130).</p> <p>NOTE: You can only select samples that have not yet been assigned to an attestation policy.</p> <p>NOTE: When you select samples, you can not set conditions anymore and vice versa.</p>
Close obsolete tasks automatically	<p>Specify whether attestation cases pending for this attestation policy are automatically closed if new attestation cases are created (for example, when there is a new attestation run of this attestation policy).</p> <p>If an attestation run with this attestation policy is started and the option is set, new attestation cases are created according to the condition. All pending, obsolete attestation cases for newly determined attestation objects of this attestation policy are stopped. Attestation cases for attestation objects that are not recalculated, remain intact.</p>
Approval by multi-factor authentication	Specify whether approvals about attestation cases governed by this attestation policy require multifactor authentication.

4. To specify which objects to attest, perform one of the following actions:
 - To add a new condition, under **Objects To Be Attested by This Attestation Policy** click **Add another condition**.
 - To edit an existing condition, under **Objects To Be Attested by This Attestation Policy**, click the condition.
 - To delete an existing condition, click  (**Delete condition**).
5. In the **Condition type** menu, click the condition type to use (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431).

NOTE: The options available in the **Condition type** menu depends on which attestation procedure is configured for the attestation policy.

6. (Optional) Depending on which condition type you have selected, you can filter the selection of objects to attest (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431).
7. (Optional) Create or modify more conditions if required. To do this, click **Add another condition**.
8. (Optional) If you have specified more than one condition, you must specify whether one or all of the conditions must be fulfilled by enabling the appropriate option:
 - **All conditions must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects fulfilling all of the conditions. If one of the objects to attest does not fulfill a condition, this object is not attested. In addition, use of this option generates a intersecting set of all the individual conditions of the selected objects.
 - **At least one condition must be fulfilled:** The next time the attestation policy is run, new attestation cases are added for all objects that fulfill at least one of the conditions. Use of this option generates a superset of all the individual conditions of the selected objects.
9. Click **Save**.

Related topics

- [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431

Copying attestation policies

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

Copied attestation policies can be deleted again.

To copy an attestation policy

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

TIP: To show disabled attestation policies, delete the **Activated attestation policies** option. To do this, click **✕** next to the filter (**Clear filter**).

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

You can edit the following main data.

Table 22: Attestation policy main data

Property	Description
Disabled	Specify whether the attestation policy is disabled or not. Attest-

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

Property	Description
Policy collection	<p>Select the policy collection to which you want to assign the attestation policy.</p> <p>To start attesting several attestation policies at the same time, you can group different attestation policies into a so-called policy collection (see Grouping attestation policies (using policy collections) on page 132).</p>
Sample	<p>Select which sampling data to use (see Running sample attestations on page 125 and Managing samples on page 130).</p> <p>NOTE: You can only select samples that have not yet been assigned to an attestation policy.</p> <p>NOTE: When you select samples, you can not set conditions anymore and vice versa.</p>
Close obsolete tasks automatically	<p>Specify whether attestation cases pending for this attestation policy are automatically closed if new attestation cases are created (for example, when there is a new attestation run of this attestation policy).</p> <p>If an attestation run with this attestation policy is started and the option is set, new attestation cases are created according to the condition. All pending, obsolete attestation cases for newly determined attestation objects of this attestation policy are stopped. Attestation cases for attestation objects that are not recalculated, remain intact.</p>
Approval by multi-factor authentication	<p>Specify whether approvals about attestation cases governed by this attestation policy require multifactor authentication.</p>

4. To specify which objects to attest, perform one of the following actions:
 - To add a new condition, under **Objects To Be Attested by This Attestation Policy** click **Add another condition**.
 - To edit an existing condition, under **Objects To Be Attested by This Attestation Policy**, click the condition.
 - To delete an existing condition, click  (**Delete condition**).
5. In the **Condition type** menu, click the condition type to use (see [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431).

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

[policies from attestation procedures](#) on page 431).

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

Related topics

- [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431

Deleting attestation policies

You can delete attestation policies that are not used anymore.

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

To delete an attestation policy

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

Starting attestation

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

| **NOTE:** You cannot start attestation with attestation policies in the **In Processing** state.

To start attestation using a scheduled task

1. In the menu bar, click **Attestation > Attestation Policies**.
2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click **✕ (Clear filter)** next to the filter.
3. Click the attestation policy that you want to start attesting.
4. In the **Edit attestation policy** pane, deselect the **Disabled** box.
5. In the **Calculation schedule** menu, specify how often an attestation run with this attestation policy is started.

Each attestation run creates a new attestation case respectively.

6. Click **Save**.

To start attestation for selected objects

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

Related topics

- [Editing attestation policies](#) on page 118
- [Running sample attestations](#) on page 125

Running sample attestations

You can perform attestations only for a subset of identities. For example, when attesting all identities would take too long. Samples contain identities that you can use to conduct a sample attestation.

To use sample data in an attestation, assign a sample to the corresponding attestation policy and start the attestation.

To run a sample attestation

1. In the menu bar, click **Attestation > Attestation Policies**.
2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click **✕ (Clear filter)** next to the filter.
3. Click the attestation policy you want to use for the sample attestation.
4. In the details pane, in the **Sample** menu, select the sample you want to use.
5. Click **Save**.
NOTE: If the attestation policy is enabled and a schedule is set up, the sample attestation is automatically carried out on the selected date and you do not need to take any further action.
6. On the **Attestation Policies** page, click **⋮ Actions > Start attestation** next to the attestation policy you want to use for the sample attestation.
7. In the **Start attestation** pane, perform one of the following actions:
 - To start attesting an object, click **Start attestation** next to the object.
 - To start attesting several objects, select the check box in front of each object and click **Start attestation for selected**.
 - To start attesting all objects, click **Start attestation for all**.

Related topics

- [Managing samples](#) on page 130

Managing attestation runs

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

Detailed information about this topic

- [Displaying attestation policy runs](#) on page 127
- [Displaying attestors of application runs](#) on page 127
- [Displaying attestation cases of application runs](#) on page 127
- [Displaying attestation run reports](#) on page 128
- [Extending attestation runs](#) on page 129
- [Sending reminders about attestation runs](#) on page 132

Displaying attestation policy runs

You can the display attestation runs of attestation policies. In addition, you can query further details for each attestation run, such as general data, attestation details, and the attestation prediction.

To display attestation policy runs

1. In the menu bar, click **Attestation > Attestation runs**.
This opens the **Attestation Policy Runs** page
2. (Optional) To display the details (current date, details about attestation, and attestation prediction) of an attestation run, click the attestation run and take the relevant details from the **View Attestation Run Details** pane on the **Details** tab.

Related topics

- [Sending reminders about attestation runs](#) on page 132

Detailed information about this topic

- [Displaying attestors of application runs](#) on page 127
- [Displaying attestation cases of application runs](#) on page 127
- [Displaying attestation run reports](#) on page 128

Displaying attestors of application runs

You can show all the attestors that still need to make approval decisions about attestation cases in an attestation run.

In addition, you can send reminders to these attestors (see [Sending reminders about attestation runs](#) on page 132).

To show attestors of an attestation run

1. In the menu bar, click **Attestation > Attestation runs**.
2. On the **Attestation Runs** page, click the attestation run whose attestor you want to display.
3. In the **View Attestation Run Details** pane, click the **Attestors** tab.

Displaying attestation cases of application runs

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

To display attestation cases of an attestation run

1. In the menu bar, click **Attestation > Attestation runs**.
2. On the **Attestation Runs** page, click the attestation run with the attestation cases you want to display.
3. In the **View Attestation Run Details** pane, click the **Attestation cases** tab.
4. (Optional) To further limit the attestation cases to be displayed, click **▼ (Filter)** on the **Attestation cases** tab (see [Filtering](#) on page 27).
5. (Optional) To display the details of an attestation case, click the attestation case and refer to the **View Attestation Case Details** pane for the relevant information.
6. (Optional) To approve or deny an attestation case, perform the following actions in the **Attestation cases** tab:
 - a. Select the check box next to the attestation case that you want to approve or deny.
 - b. Click **Approve** or **Deny**.
 - c. In the **Approve Attestation Case/Deny Attestation Case** pane, enter a reason for your approval decision in the **Reason for decision** field.
 - d. In the **Additional comments about your decision** field, enter extra information about your approval decision.
 - e. Click **Save**.

Related topics

- [Displaying pending attestation cases](#) on page 137
- [Approving or denying attestation cases](#) on page 138

Displaying attestation run reports

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

To display an attestation run's report

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

Related topics

- [Displaying attestation policy reports](#) on page 115

Extending attestation runs

You can extend attestation runs.

To extend an attestation run

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

Related topics

- [Sending reminders about attestation runs](#) on page 132

Attestation by peer group analysis

Using peer group analysis, approval for attestation cases can be granted or denied automatically. For example, a peer group might be all identities in the same department. Peer group analysis assumes that these identities require the same products. For example, if the majority of identities belonging to a department have a particular product, assignment to another identity in the department can be approved automatically. This helps to accelerate approval processes.

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

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

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

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

Related topics

- [Appendix: Attestation conditions and approval policies from attestation procedures](#) on page 431

Managing samples

You can perform attestations only for a subset of identities. For example, when attesting all identities would take too long. Samples contain identities that you can use to conduct a sample attestation.

TIP: To use samples in an attestation, assign a sample to the corresponding attestation policy and start the attestation (see [Running sample attestations](#) on page 125).

Detailed information about this topic

- [Displaying samples](#) on page 130
- [Creating samples](#) on page 130
- [Editing samples](#) on page 131
- [Deleting samples](#) on page 131

Displaying samples

To obtain an overview, you can display samples.

To display samples

1. In the menu bar, click **Attestation > Sample data**.
This opens the **Sample Data** page.
2. (Optional) To view the sample data of a sample, click the sample.

Creating samples

You can create new samples. To do this, you create a sample and assign the corresponding sample data to it.

To create a sample

1. In the menu bar, click **Attestation > Sample data**.
2. On the **Sample Data** page, click **+ Create sample**.
3. In the **Create sample** pane, enter a name for the sample in the **Display name** field.
4. Click **Next**.
5. In the **Assign identities** step, select the check box in front of the identity to which you want to assign the sample.

TIP: To create an empty sample, do not select a check box and click **Skip**. You can assign identities to the sample later by editing it.

6. Click **Next**.
7. In the **Summary** step, click **Save**.

Editing samples

You can assign additional identities to existing samples or remove them.

To assign another identity to a sample

1. In the menu bar, click **Attestation > Sample data**.
2. On the **Sample Data** page, click the sample you want to edit.
3. In the **Edit Sample** pane, click **Assign identities**.
4. In the **Select Identities** pane, select the check box next to the identity you want to assign to the samples.
5. Click **Assign**.

To remove an identity from a sample

1. In the menu bar, click **Attestation > Sample data**.
2. On the **Sample Data** page, click the sample you want to edit.
3. In the **Edit Sample** pane, select the check box next to the identity you want to remove.
4. Click **Remove identities**.
5. In the **Remove Identities** dialog, confirm the prompt with **Yes**.

Deleting samples

You can delete existing samples.

To delete a sample

1. In the menu bar, click **Attestation > Sample data**.
2. On the **Sample Data** page, select the check box next to the sample you want to delete.
TIP: To delete multiple samples, select additional check boxes in front of the respective samples.
3. Click **Delete**.
4. In the **Delete Sample** dialog, confirm the prompt with **Yes**.

Sending attestation reminders

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

- You can send reminders to attestors of attestation cases that belong to certain attestation runs (see [Sending reminders about attestation runs](#) on page 132).

Sending reminders about attestation runs

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

To send a reminder to all attestors of all attestation runs

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

To send a reminder to attestors of a selected attestation run

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

Grouping attestation policies (using policy collections)

To start attesting multiple attestation policies at the same time, you can group different attestation policies into a so-called policy collection. For example, this can be used in the

context of an audit, when different attestations are run that have related content.

The following policies apply to policy collections:

- You can assign an attestation policy to just one policy collection.
- You cannot start attestation policies that belong to a policy collection separately.
- When samples are attested, the same sample is used for all the attestation policies that belong to one policy collection.

Detailed information about this topic

- [Displaying policy collections](#) on page 133
- [Creating policy collections](#) on page 133
- [Editing policy collections](#) on page 134
- [Disabling policy collections](#) on page 135
- [Deleting policy collections](#) on page 136
- [Assigning policy collections to attestation policies](#) on page 136

Displaying policy collections

To obtain an overview, you can display policy collections.

To display policy collections

1. In the menu bar, click **Attestation > Policy collections**.
This opens the **Policy Collections** page.
2. (Optional) To display the main data of a policy collection, click the policy collection.

Creating policy collections

You can create a policy collection. You can then assign attestation policies to the policy collection that you want to be grouped together and started at the same time (see [Setting up attestation policies](#) on page 116 and [Editing attestation policies](#) on page 118).

To create a policy collection

1. In the menu bar, click **Attestation > Policy collections**.
2. On the **Policy Collections** page, click **+ Create policy collection**.
3. On the **Create Policy Collection** pane, enter the main data of the policy collection.

You can edit the following main data.

Table 23: Policy collection main data

Property	Description
Policy collection	Enter a name for the policy collection.
Description	Enter a description of the policy collection.
Disabled	Select the check box to disable all the associated attestation polices. Thus, no attestations are carried out on the policy collection.
Owner (application role)	Click Select and then the application role whose members can manage the policy collection.
Calculation schedule	Define how often an attestation run is started with the associated attestation policies. Each attestation run creates a new attestation case respectively.
Owners	Select the identity that is responsible for this policy collection. This identity can manage the policy collection.
Sample	Select which sampling data to use (see Running sample attestations on page 125). Use a sample to limit the set of objects to attest for all assigned attestation policies. NOTE: You can only select samples that have not yet been assigned to a policy collection.

4. Click **Create**.

Editing policy collections

You can edit the main data of policy collections.

To delete a policy collection

1. In the menu bar, click **Attestation > Policy collections**.
2. On the **Policy Collections** page, click the policy collection that you want to edit.
3. On the **Edit Policy Collection** pane, enter the main data of the policy collection.

You can edit the following main data.

Table 24: Policy collection main data

Property	Description
Policy collection	Enter a name for the policy collection.
Description	Enter a description of the policy collection.
Deactivated	Select the check box to disable all the associated attestation policies. Thus, no attestations are carried out on the policy collection.
Owner (application role)	Click Select and then the application role whose members can manage the policy collection.
Calculation schedule	Define how often an attestation run is started with the associated attestation policies. Each attestation run creates a new attestation case respectively.
Owners	Select the identity that is responsible for this policy collection. This identity can manage the policy collection.
Sample	Select which sampling data to use (see Running sample attestations on page 125). Use a sample to limit the set of objects to attest for all assigned attestation policies. NOTE: You can only select samples that have not yet been assigned to a policy collection.

4. Click **Save**.

Disabling policy collections

To prevent attestations being run for policy collections, you can disable policy collections. This also disables all associated attestation policies and deletes their attestation cases.

To disable a policy collection

1. In the menu bar, click **Attestation > Policy collections**.
2. On the **Policy Collections** page, click the policy collection that you want to disable.
3. In the **Edit Policy Collection** pane, select the **Disable** check box.
4. Click **Save**.

Deleting policy collections

You can delete policy collections.

To delete a policy collection

1. In the menu bar, click **Attestation > Policy collections**.
2. On the **Policy Collections** page, next to the policy collection you want to delete, click  **Delete**.
3. In the **Delete Policy Collection** dialog, confirm the prompt with **Yes**.

Assigning policy collections to attestation policies

To group attestation policies together, you can assign multiple attestation policies to a specific policy collection.

To assign an attestation policy to a policy collection.

1. In the menu bar, click **Attestation > Attestation Policies**.
2. On the **Attestation Policies** page, click the attestation policy you want to assign to a policy collection.
TIP: To show disabled attestation policies, delete the **Activated attestation policies** option. To do this, click  (**Clear filter**) next to the filter.
3. In the **Edit Attestation Policy** pane, in the **Policy collection** menu, select the policy collection to which you want to assign the attestation policy.
4. Click **Save**.

Pending attestations

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

Detailed information about this topic

- [Displaying pending attestation cases](#) on page 137
- [Approving or denying attestation cases](#) on page 138
- [Appointing other approvers for pending attestation cases](#) on page 139
- [Rejecting approval of attestation cases](#) on page 144
- [Managing inquiries about pending attestation cases](#) on page 145

Displaying pending attestation cases

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

To display pending attestation cases

1. In the menu bar, click **Attestation > Pending Attestations**.
This opens the **Pending Attestations** page.
2. (Optional) On the **Pending attestations** page, perform one of the following actions:
 - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
 - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. (Optional) To show more details of an attestation case, click the attestation case.
4. (Optional) To display all the identities that can approve an attestation case, perform the following actions:
 - a. Click the attestation case.
 - b. In the **View Attestation Case Details** pane, click the **Workflow** tab.
5. (Optional) To display rule violations of an attestation case, perform the following actions:
 - a. Click the attestation case.
 - b. In the **View Attestation Case Details** pane, click the **Rule Violations** tab.
 - c. (Optional) To assign mitigating controls to the rule violation, on the **Rule Violations** tab, click **Edit mitigating controls** and assign an appropriate mitigating control.
6. (Optional) To display policy violations of an attestation case, perform the following actions:
 - a. Click the attestation case.
 - b. In the **View Attestation Case Details** pane, click the **Policy Violations** tab.
 - c. (Optional) To assign mitigating controls to the policy violation, on the **Rule Violations** tab, click **Edit mitigating controls** and assign an appropriate mitigating control.

Related topics

- [Displaying attestation cases of application runs](#) on page 127

Approving or denying attestation cases

As attestor, you can approve or deny attestation cases under your supervision.

To make an approval decision about an attestation case

1. In the menu bar, click **Attestation > Pending Attestations**.
2. (Optional) On the **Pending attestations** page, perform one of the following actions:
 - To display attestation cases of a specific object, click **▼ (Filter)** and in the context menu, select the corresponding object under **Object type**.
 - To display attestation cases of a specific attestation policy, click **▼ (Filter)** and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. (Optional) To approve an attestation case as a member of the chief approval team and only display the relevant attestation cases, toggle the **Show attestation cases to be approved by chief approval team** switch.
4. Perform one of the following actions:
 - To approve an attestation case, click **✓ Approve** next to the attestation case.
 - To deny an attestation case, click **⊗ Deny** next to the attestation case.

TIP: To approve or deny multiple attestation cases, in the list, select the check boxes next to the attestation cases and click **Approve** or **Deny** below the list.

5. In the **Approve Attestation Case/Deny Attestation Case** pane, perform the following actions:
 - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
 - b. In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

NOTE: For more detailed information about standard reasons, see the [One Identity Manager IT Shop Administration Guide](#).

6. Click **Save**.

Related topics

- [Displaying attestation cases of application runs](#) on page 127

Appointing other approvers for pending attestation cases

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

- **Reroute approval**
You give the task of approving to another approval level (see [Rerouting approvals of pending attestation cases](#) on page 139).
- **Appoint additional approver**
You delegate the task of approving to another identity (see [Appointing additional approvers to pending attestation cases](#) on page 140). The additional approver must make an approval decision in addition to the other approvers. The additional approver can reject the approval and return it to you (see [Rejecting approval of attestation cases](#) on page 144). You can withdraw an additional approver. For example, if the other approver is not available.
- **Delegate approval**
You delegate the task of approving to another approval level (see [Delegating approvals of pending attestation cases to other identities](#) on page 142). This identity is added as approver in the current approval step and makes approval decisions on your behalf. The new approver can reject the approval and return it to you (see [Rejecting approval of attestation cases](#) on page 144). You can withdraw a delegation and delegate another identity. For example, if the other approver is not available.

Rerouting approvals of pending attestation cases

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

To reroute an approval

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

3. On the **Pending Attestations** page, click the attestation case whose approval you want to reroute.
4. In the **View Attestation Case Details** pane, click **Reroute approval**.
5. In the **Reroute approval** pane, in the **Select approval level** menu, select the approval level you want to reroute to.
6. (Optional) In the **Reason for your decision** field, enter a reason for rerouting.
7. Click **Save**.

To reroute multiple approvals

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

Appointing additional approvers to pending attestation cases

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

To add an additional approver

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

3. On the **Pending Attestations** page, click the attestation case to which you want to add an additional approver.
4. In the **View Attestation Case Details** pane, click **Add attestor**.
5. In the **Add Additional Attestor** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.
6. In the **Reason for your decision** field, select a standard reason for adding an additional approver.
7. Click **Save**.

To add an additional approver to multiple attestation cases

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

Related topics

- [Removing additional approvers from pending attestation cases](#) on page 141

Removing additional approvers from pending attestation cases

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

To withdraw an attestation case's additional approver

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

- To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu, select the corresponding object under **Object type**.
 - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu, select the corresponding attestation policy under **Attestation policy**.
3. On the **Pending Attestations** page, click the attestation case to which you added an additional approver.
 4. In the **View Attestation Case Details** pane, click **Withdraw additional attestor**.
 5. In the **Withdraw Additional Attestor** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.
 6. Click **Save**.

To withdraw an additional approver from multiple attestation cases

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

Related topics

- [Appointing additional approvers to pending attestation cases](#) on page 140

Delegating approvals of pending attestation cases to other identities

You can delegate an approval decision about an attestation case to another identity. You can revoke this action in the attestation history (see [Withdrawing delegations from pending attestation case approvals](#) on page 143).

To delegate an approval

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

To delegate approval of multiple attestation cases

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

Related topics

- [Withdrawing delegations from pending attestation case approvals](#) on page 143

Withdrawing delegations from pending attestation case approvals

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

To withdraw an approval delegation

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

To withdraw multiple delegations from approvals

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

Related topics

- [Delegating approvals of pending attestation cases to other identities](#) on page 142

Rejecting approval of attestation cases

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

To reject an approval

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

5. In the **Reject Approval** pane, in the **Reason for your decision** pane, enter a reason for the rejecting.
6. Click **Save**.

To reject approval of multiple attestation cases

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

Managing inquiries about pending attestation cases

To gather information about pending attestation cases, you can send inquiries about them to any identity.

Once you have sent an inquiry about an attestation case, the attestation case is reserved for you (Hold status). As long as the attestation case is reserved for you, only you or the chief approval team can make an approval decision about the attestation case. You can withdraw the inquiry at any time. You can cancel the reservation at any time so that another approver can make approval decision about the attestation case.

Related topics

- [Managing attestation inquiries directed at you](#) on page 149
- [Managing inquiries about pending requests](#) on page 103

Detailed information about this topic

- [Submitting inquiries about pending attestation cases](#) on page 146
- [Withdrawing inquiries about pending attestation cases](#) on page 146
- [Revoking reserved attestation cases](#) on page 147
- [Displaying answers to inquiries about pending attestation cases](#) on page 147

Submitting inquiries about pending attestation cases

Before you make an approval decision about an attestation case, you can send a question to an identity about it.

NOTE: Once you have sent an inquiry about an attestation case, the attestation case is reserved for you (Hold status). As long as the request is reserved for you, only you or the chief approval team can make an approval decision about the attestation case.

You can revoke the reservation with the following actions:

- Withdraw the inquiry (see [Withdrawing inquiries about pending attestation cases](#) on page 146)
- Cancel the reservation (see [Revoking reserved attestation cases](#) on page 147)

To make an inquiry

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, click the attestation case that you want to inquire about.
3. In the **View Attestation Case Details** pane, click **Send inquiry**.
4. In the **Send Inquiry** pane, in the **Recipient of the inquiry** menu, select the identity to which you want to send the inquiry.
5. In the **Inquiry** field, enter your inquiry.
6. Click **Save**.

Related topics

- [Managing attestation inquiries directed at you](#) on page 149

Withdrawing inquiries about pending attestation cases

If your issue with an attestation case has become irrelevant, you can withdraw your inquiry again. Once you have withdrawn the inquiry, the attestation case reservation is also revoked and all the original approvers can approve the attestation case again.

To withdraw and inquiry

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, click the attestation case that you inquired about.
3. In the **View Attestation Case Details** pane, click **Withdraw inquiry**.

4. (Optional) In the **Withdraw Inquiry** pane, in the **Reason for your decision** field, enter why you are withdrawing the inquiry.
5. Click **Save**.

Related topics

- [Managing attestation inquiries directed at you](#) on page 149

Revoking reserved attestation cases

Once you have sent an inquiry about an attestation case, the attestation case is reserved for you (Hold status). As long as the attestation case is reserved for you, only you or the chief approval team can make an approval decision about the attestation case.

To release the attestation case again for attestation and to allow other approvers to edit it, you can revoke the reservation with the following actions:

- You can withdraw the inquiry (see [Withdrawing inquiries about pending attestation cases](#) on page 146).
- You can cancel the inquiry manually.

To cancel a reservation

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, click the attestation case that you inquired about.
3. In the **View Attestation Case Details** pane, click **Cancel reservation**.
4. (Optional) In the **Cancel Reservation** pane, in the **Reason for your decision**, enter a reason for canceling the reservation.
5. Click **Save**.

Related topics

- [Managing attestation inquiries directed at you](#) on page 149

Displaying answers to inquiries about pending attestation cases

If the identity you sent an inquiry to has responded to it, you can view their answer in the workflow of the respective attestation case.

To display an answer

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, click the attestation case that you inquired about.
3. In the **View Attestation Case Details** pane, click the **Workflow** tab.
In the workflow, the response is displayed under **Answer**.

Related topics

- [Managing attestation inquiries directed at you](#) on page 149

Displaying attestation history

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

To display the attestation history

1. In the menu bar, click **Attestation > Attestation history**.
This opens the **Attestation History** page.
2. Perform one of the following actions:
 - To display attestation cases of a specific object, click ▼ (**Filter**) and in the context menu under **Object type**, select the corresponding object.
 - To display attestation cases of a specific attestation policy, click ▼ (**Filter**) and in the context menu under **Object type**, select the corresponding attestation policy.
 - To display an attestation case of a specific object, click ▼ (**Filter**) and in the context menu in the **Attestor** menu, select the relevant identity.
3. (Optional) To control which attestation cases are displayed, click ▼ (**Filter**) (see [Filtering](#) on page 27). For example, this allows you to show just pending attestation cases (no approval decision yet made).
4. (Optional) To display details of an attestation case, click the attestation case whose details you want to display.

Related topics

- [Withdrawing delegations from pending attestation case approvals](#) on page 143

Managing attestation inquiries directed at you

To gather further information about a pending attestation case is approved, the approver can send you a question about this attestation case. After you have answered the inquiry, the approver can make their approval decision.

Related topics

- [Managing inquiries about pending attestation cases](#) on page 145
- [Managing request inquiries directed at you](#) on page 111

Detailed information about this topic

- [Displaying attestation case inquiries](#) on page 149
- [Answering attestation case inquiries](#) on page 149

Displaying attestation case inquiries

You can display inquiries about an attestation case that have been sent to you and to which you must respond.

To view inquiries directed at you

1. In the menu bar, click **Attestation** > **Pending Attestations**.
2. On the **Pending Attestations** page, click the **Inquiries** tab.
3. (Optional) To see more information about the answer to an attestation case inquiry, click the respective inquiry.

Related topics

- [Managing inquiries about pending attestation cases](#) on page 145

Answering attestation case inquiries

You can respond to inquiries that have been made to you about an attestation case.

TIP: If you respond to inquiries, do not grant or deny approval for the attestation case.

To respond to inquiries

1. In the menu bar, click **Attestation > Pending Attestations**.
2. On the **Pending Attestations** page, click the **Inquiries** tab.
3. On the **Inquiries** tab, next to the inquiry you want to answer, click the **Reply to inquiry**.
4. In the **Answer Question** pane, enter your answer in the **Reply to inquiry** field.
5. Click **Save**.

Related topics

- [Submitting inquiries about pending attestation cases](#) on page 146

Compliance

Companies have different requirements that they need for regulating internal and external identities' access to company resources. On the one hand, rule checks are used for locating rule violations and on the other hand, to prevent them. By using these rules, you can demonstrate compliance with legislated regulations such as the Sarbanes-Oxley Act (SOX). The following demands are made on compliance:

- Compliance rules define what an identity is entitled to do or not do. For example, an identity may not have both entitlements A and B at the same time.
- Company policies are very flexible, and can be defined for any company resources you are managing with Manager. For example, a policy might only allow identities from a certain department to own a certain entitlement.
- Each item that an identity can access, can be given a risk value. A risk index can be calculated for identities, accounts, organization, roles, and for the groups of resources available for request. You can then use the risk indexes to help prioritize your compliance activities.

Some rules are preventative. For example, a request will not be processed if it violates the rules, unless exception approval is explicitly granted and an approver allows it. Compliance rules (if appropriate) and company policies are run on a regular schedule, and violations appear in the identity's Web Portal to be dealt with there. Company policies can contribute to mitigation control by reducing risk. For example, if risks are posed by identities running processes outside the One Identity Manager solution and causing violations. Reports and dashboards provide you with comprehensive compliance information

Detailed information about this topic

- [Displaying compliance rules](#) on page 152
- [Managing company policies](#) on page 158

Managing compliance rules

One Identity Manager can be used to define rules that maintain and monitor regulatory requirements and automatically deal with rule violations. Define compliance rules to test

entitlements or combinations of entitlements in the context of identity audit for identities in the company. On the one hand, existing rule violations can be found by checking rules. On the other hand, possible rule violations can be preemptively identified and thus prevented.

For more information about compliance rules, see the *One Identity Manager Compliance Rules Administration Guide*.

Detailed information about this topic

- [Displaying compliance rules](#) on page 152
- [Displaying reports about compliance rules and rule violations](#) on page 154
- [Check compliance rules and find rule violations](#) on page 155
- [Managing rule violations](#) on page 155

Displaying compliance rules

You can display a overview of compliance rules.

To display all compliance rules

1. In the menu bar, click **Compliance > Compliance rules**.
This opens the **Compliance rules** page.
2. (Optional) To further limit or extend which compliance rules are displayed, click ▼ (**Filter**) and in the context menu, under **Status**, select one of the following filters:
 - **Activated**: Select this filter to display only enabled compliance rules.
 - **Deactivated**: Select this filter to display only disabled compliance rules.

TIP: To view all the compliance rules, clear the filter. To do this, click **Clear filters** on the context menu.
3. (Optional) To display details of a compliance rule, click the corresponding compliance rule.

Detailed information about this topic

- [Displaying rule violations of compliance rules](#) on page 152
- [Displaying mitigating controls of compliance rules](#) on page 153
- [Displaying compliance rule statistics](#) on page 153
- [Displaying compliance rule hyperviews](#) on page 154

Displaying rule violations of compliance rules

You can display the rule violations of certain compliance rules. This information can help to determine gaps in your security or compliance policies and to develop attestation policies

or mitigating controls.

TIP: For more information about displaying rule violations that you can approve, see [Displaying approvable rule violations](#) on page 155.

To display the rule violations of a compliance rule

1. In the menu bar, click **Compliance > Compliance rules**.
2. On the **Compliance Rules** page, click the compliance rule whose rule violations you want to display.
3. In the **View Compliance Rule Details** pane, click the **Rule violations** tab.
4. (Optional) To display details of a rule violation, click the appropriate rule violation.

Related topics

- [Managing rule violations](#) on page 155

Displaying mitigating controls of compliance rules

You can display the mitigating controls of certain compliance rules.

The following options are available depending on the system configuration.

- The mitigation controls displayed are automatically assigned to all the rule violations of the corresponding compliance rule.
- The mitigation controls displayed can be assigned individually to rule violations of the corresponding compliance rule (see [Assigning mitigating controls to rule violations](#) on page 156).

Mitigating controls are processes existing outside the One Identity Manager solution and reduce the risk of violation.

To display the mitigating controls of a compliance rule

1. In the menu bar, click **Compliance > Compliance rules**.
2. On the **Compliance Rules** page, click the compliance rule whose mitigating controls you want to display.
3. In the **View Compliance Rule Details** pane, click the **Mitigating Controls** tab.

Displaying compliance rule statistics

You can display the statistics of certain compliance rules.

To display the statistics of a compliance rule

1. In the menu bar, click **Compliance > Compliance rules**.
2. On the **Compliance Rules** page, click the compliance rule whose statistics you want to display.
3. In the **View Compliance Rule Details** pane, click the **Statistics** tab.

Displaying compliance rule hyperviews

To quickly grasp dependencies and relationships of compliance rules, you can display compliance rule data in a Hyperview view at any time.

To display the Hyperview of an compliance rule

1. In the menu bar, click **Compliance > Compliance rules**.
2. On the **Compliance Rules** page, click the compliance rule whose overview you want to display.
3. In the **View Compliance Rule Details** pane, click the **Hyperview** tab.

Displaying reports about compliance rules and rule violations

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).

To display a report about a compliance rule and its rule violations

1. In the menu bar, click **Compliance > Compliance rules**.
2. (Optional) To further limit or extend which compliance rules are displayed, on the **Compliance Rules** page, click **▼ (Filter)** and in the context menu, under **Status**, select one of the following filters:
 - **Activated:** Select this filter to display only enabled compliance rules.
 - **Deactivated:** Select this filter to display only disabled compliance rules.

TIP: To view all compliance rules, clear the filter. To do this, click **Clear filters** on the context menu.
3. Click the compliance rule about which you want to display a report.
4. In the **View Compliance Rule Details** pane, click **Download report**.

Check compliance rules and find rule violations

To determine whether there are rule violations, you can check the compliance rules. To do this, start a recalculation of the respective compliance rules.

To recalculate a compliance rule

1. In the menu bar, click **Compliance > Compliance rules**.
2. On the **Compliance Rules** page, next to the compliance rule you want to recalculate, click **Recalculate**.

Managing rule violations

Compliance rules that are violated generate rule violations. Rule violation exceptions can be granted or denied.

Detailed information about this topic

- [Displaying approvable rule violations](#) on page 155
- [Assigning mitigating controls to rule violations](#) on page 156
- [Granting and denying rule violation exceptions](#) on page 156
- [Resolving rule violations](#) on page 157

Displaying approvable rule violations

You can display rule violations that you can approve. In doing so, you can additionally display rule violations that already have an approval decision.

To display rule violations

1. In the menu bar, click **Compliance > Rule violations**.
This opens the **Rule Violations** page and displays all the rule violations that are still subject to approval.
2. (Optional) To display rule violations that have already been approved or denied, click **▼ (Filter)** and enable the corresponding option in the menu.
3. (Optional) To display details of a rule violation, click the appropriate rule violation.

Related topics

- [Displaying my identities' rule violations](#) on page 234
- [Displaying rule violations of compliance rules](#) on page 152

Assigning mitigating controls to rule violations

Mitigating controls can be assigned to rule violations to reduce the risk of rule violations.

NOTE: You can assign only mitigating controls that are also assigned to the compliance rules that are violated.

NOTE: You can only assign mitigating controls to a rule violation if your system is configured appropriately. Otherwise, the mitigating controls assigned to the compliance rule are automatically assigned to every other related rule violation.

To assign mitigating controls to a rule violation

1. In the menu bar, click **Compliance > Rule violations**.
2. On the **Rule Violations** page, click the rule violation to which you want to assign mitigating controls.
3. In the **View Rule Violation Details** pane, click the **Mitigating Controls** tab.
4. On the **Mitigating Controls** tab, click **Assign mitigating controls**.
5. In the menu, select the mitigating control that you want to assign to the rule violation.
6. (Optional) To assign other mitigating controls, click **+** (**Assign mitigating control**).
7. Click **Save**.

Granting and denying rule violation exceptions

As exception approver, you can grant or deny exception approval to rule violations.

To make an approval decision about a rule violation

1. In the menu bar, click **Compliance > Rule violations**.
2. On the **Rule Violations** page, perform one of the following actions:
 - To grant an exception for a rule violation, next to the rule violation, click **Grant exception**.
 - To deny an exception for a rule violation, next to the rule violation, click **Deny exception**.

TIP: To grant or deny exceptions to several rule violations at the same time, select the check box next to each rule violation and click **Grant exception** or **Deny exception** at the bottom of the list.

3. (Optional) To set an approval deadline, in the **Grant exception/Deny exception** pane, in the **Valid until** field, enter a date and time.
 4. (Optional) Perform the following actions:
 - a. In the **Reason for your decision** menu, select a standard reason for your approval decision.
 - b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.
- TIP:** By giving reasons, your approvals are more transparent and support the audit trail.
- NOTE:** For more detailed information about standard reasons, see the One Identity Manager Compliance Rules Administration Guide.
5. Click **Save**.

Resolving rule violations

You can resolve compliance rule violations that you manage. Rule violations are caused by entitlements, so you have the option to remove entitlements when you want to resolve one.

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

The following consequences may result from removing entitlements:

Table 25: Removing assigned entitlements

Assignment method	Removing the entitlement
Direct assignment	Direct assignment is deleted when the entitlement is removed.
Inherited assignment	In the case of inherited entitlements, there is an option provided to withdraw role membership from the identity.
Dynamic assignment	Entitlements that were assigned automatically through a dynamic role cannot be removed.
Assignment by request	If entitlements were assigned through a request, the request is broken off if the entitlements are removed.
Primary assignment	If entitlements were assigned through a primary membership, the identity of the primary membership can be optionally revoked if the entitlements are removed.

To resolve a rule violation

1. In the menu bar, click **Compliance > Rule violations**.
2. On the **Rule Violations** page, click the rule violation you would like to resolve.
3. In the **View Rule Violation Details** pane, click **Resolve rule violation**.
This opens the **Resolve Rule Violation** pane and shows you more details about the rule violation and the entitlements that lead to the rule violation.
4. Select the check box next to the entitlement you want to be withdrawn from the identity.
5. Click **Next**.
6. In the **Verify actions** step, check the changes that should be performed and, if necessary, clear the check boxes in front of the actions that you do not want performed.
7. Click **Continue**.
8. In the **Loss of entitlements check** step, check which entitlements are withdrawn from the user to avoid unintentional loss of entitlements.
9. Click **Next**.

Managing company policies

Companies have varying requirements that they need for regulating access of internal and external identities to company resources. They also have to demonstrate that they adhere to legal requirements. Such requirements can be defined as company policies.

One Identity Manager allows you to manage these company policies and thus assess the risk involved. Assuming the appropriate data is stored in the One Identity Manager database, One Identity Manager determines all the company resources that violate these company policies. You can also define company policies for the purpose of providing reports that do not have any connection with One Identity Manager.

For more information about company policies, see the *One Identity Manager Company Policies Administration Guide*.

Detailed information about this topic

- [Managing policy violations](#) on page 161

Displaying company policies

You can display an overview of company policies.

To display all company policies

1. In the menu bar, click **Compliance > Company policies**.
This opens the **Company Policies** page.
2. (Optional) To further limit or extend which company policies are displayed, click **Filter** and in the context menu, under **Status**, select one of the following filters:
 - **Activated**: Select this filter to display only enabled company policies.
 - **Deactivated**: Select this filter to display only disabled company policies.

TIP: To view all the company policies, clear the filter. To do this, click **Clear filters** on the context menu.
3. (Optional) To display details of a compliance rule, click the corresponding compliance rule.

Detailed information about this topic

- [Displaying policy violations of company policies](#) on page 159
- [Displaying mitigating controls of company policies](#) on page 160
- [Displaying company policy statistics](#) on page 160
- [Displaying company policy hyperviews](#) on page 160

Displaying policy violations of company policies

You can display the policy violations of certain company policies. This information can help to determine gaps in your security or compliance policies and to develop attestation policies or mitigating controls.

TIP: For more information about displaying policy violations that you can approve, see [Displaying approvable policy violations](#) on page 161.

To display the policy violations of a company policy

1. In the menu bar, click **Compliance > Company policies**.
2. On the **Company Policies** page, click the company policy whose policy violations you want to display.
3. In the **View Company Policy Details** pane, click the **Policy violations** tab.
4. (Optional) To display details of a policy violation, click the appropriate policy violation.

Related topics

- [Managing policy violations](#) on page 161

Displaying mitigating controls of company policies

You can display the mitigating controls of certain company policies.

The following options are available depending on the system configuration.

- The mitigation controls displayed are automatically assigned to all the policy violations of the corresponding company policy.
- The mitigation controls displayed can be assigned individually to policy violations of the corresponding company rule (see [Assigning mitigating controls to rule violations](#) on page 156).

Mitigating controls are processes existing outside the One Identity Manager solution and reduce the risk of violation.

To display the mitigating controls of a company rule

1. In the menu bar, click **Compliance > Company policies**.
2. On the **Company Policies** page, click the company policy whose mitigating controls you want to display.
3. In the **View Company Policy Details** pane, click the **Mitigating Controls** tab.

Displaying company policy statistics

You can display the statistics of certain company policies.

To display the statistics of a company policy

1. In the menu bar, click **Compliance > Company policies**.
2. On the **Company Policies** page, click the company policy whose statistics you want to display.
3. In the **View Company Policy Details** pane, click the **Statistics** tab.

Displaying company policy hyperviews

To quickly grasp company policy dependencies and relationships, you can view company policy data in a Hyperview view at any time.

To display the Hyperview of a company policy

1. In the menu bar, click **Compliance > Company policies**.
2. On the **Company Policies** page, click the company policy whose overview you want to display.
3. In the **View Company Policy Details** pane, click the **Hyperview** tab.

Managing policy violations

Company policies that are violated generate policy violations. Policy violations may be approved as an exception.

Detailed information about this topic

- [Displaying approvable policy violations](#) on page 161
- [Assigning mitigating controls to policy violations](#) on page 161
- [Granting and denying rule violation exceptions](#) on page 156

Displaying approvable policy violations

You can display rule violations that you can approve. In doing so, you can additionally display policy violations that already have an approval decision.

To display policy violations

1. In the menu bar, click **Compliance > Policy violations**.
This opens the **Policy Violations** page and displays all the policy violations.
2. (Optional) To control which policy violations are displayed, click ▼ (**Filter**) and enable the corresponding option in the context menu.
3. (Optional) To display details of a policy violation, click the appropriate policy violation.

Related topics

- [Displaying policy violations of company policies](#) on page 159

Assigning mitigating controls to policy violations

Mitigating controls can be assigned to policy violations to reduce the risk of policy violations.

NOTE: You can assign only mitigating controls that are also assigned to the company policies that are violated.

NOTE: You can only assign mitigating controls to a policy violation if your system is configured appropriately. Otherwise, the mitigating controls assigned to the policy violation are automatically assigned to every other related policy violation.

To assign mitigating controls to a policy violation

1. In the menu bar, click **Compliance > Policy violations**.
2. On the **Policy Violations** page, click the policy violation to which you want to assign mitigating controls.
3. In the **View Policy Violation Details** pane, click the **Mitigating Controls** tab.
4. On the **Mitigating Controls** tab, click **Assign mitigating controls**.
5. In the menu, select the mitigating control that you want to assign to the policy violation.
6. (Optional) To assign other mitigating controls, click **+ (Assign mitigating control)**.
7. Click **Save**.

Granting and denying policy violation exceptions

As exception approver, you can grant or deny exception approval to policy violations.

To make an approval decision about a policy violation

1. In the menu bar, click **Compliance > Policy violations**.
2. On the **Policy Violations** page, perform one of the following actions:
 - To grant an exception for a policy violation, next to the policy violation, click **Grant exception**.
 - To deny an exception for a policy violation, next to the policy violation, click **Deny exception**.

TIP: To grant or deny exceptions to several policy violations at the same time, select the check box next to each policy violation and click **Grant Exception** or **Deny Exception** below the list.

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

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

NOTE: For more detailed information about standard reasons, see the One Identity Manager Company Policies Administration Guide.

4. Click **Save**.

Managing risk index functions

Everyone with IT system authorization in a company represents a security risk for that company. For example, an identity with permission to edit financial data in SAP carries a higher risk than an identity with permission to edit their own main data. To quantify the risk, you can enter a risk value for every company resource in One Identity Manager. A risk index is calculated from this value for every identity that has this company resource assigned to it directly or indirectly. Company resources include target system entitlements (for example, Active Directory groups or SAP profiles), system roles, subscribable reports, software, and resources. In this way, all the people that represent a particular risk to the company can be found.

In the context of Identity Audit, compliance rules can also be given a risk index. With each rule violation, the security risk of all identities that violate the rule may increase. Therefore, these risk indexes are also included in the identities' risk calculation. You can define appropriate countermeasures through mitigating controls, and store them with the compliance rules.

Other factors can influence the calculation of identities' risk indexes. These include: the type of resource assignment (approved request or direct assignment), attestations, exception approvals for rule violations, identities' responsibilities, and defined weightings. Furthermore, the risk index can be calculated for all business roles, organizations, and system roles that have company resources assigned to them. The user account risk index is calculated based on the system entitlements assigned.

Based on the risk index history, resulting risk indexes are calculated for employees, user accounts, and hierarchical roles. All direct and indirectly assigned objects are taken into account.

One Identity Manager provides default risk index functions for risk indexes, which define the risk calculation for different types of objects. Certain properties of default risk index functions can be edited in One Identity Manager. You can also set up custom risk index functions.

For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Detailed information about this topic

- [Displaying risk index functions](#) on page 164
- [Editing risk index functions](#) on page 164

- [Disabling/enabling risk index functions](#) on page 166
- [Starting risk index calculation manually](#) on page 166

Displaying risk index functions

To obtain an overview, you can display risk index functions that contribute to the calculation of the risk index of all assigned company resources.

To display all risk index functions

1. In the menu bar, click **Setup > Risk index functions**.
This opens the **Risk Index functions** page.
2. (Optional) To display the main data of a risk index function, click the risk index function.

Editing risk index functions

You can edit risk index functions that contribute to the calculation of the risk index of all assigned company resources.

To edit a risk index function

1. In the menu bar, click **Setup > Risk index functions**.
2. On the **Risk Index Functions** page, click the risk index function you want to edit.
3. In the **Edit Risk Index Functions** pane, edit the main data of the risk index function.

You can edit the following main data.

Table 26: Risk index function main data

Property	Description
Description	Enter a description of the risk index function.
Calculate immediately	Select the check box to ensure that the risk index is calculated immediately. If you clear the check box, calculation is triggered asynchronously via the DBQueue processor.
Disabled	Select this check box if you do not want the risk index function to be taken into account in the overall the calculation of the risk indexes (see Disabling/enabling risk index functions on page 166).
Calculation type	<p>Select the calculation type to be used for calculating the risk index:</p> <ul style="list-style-type: none"> • Maximum (weighted): The highest value from all relevant risk indexes is determined, weighted and used as the basis for further calculation. • Maximum (normalized): The highest value from all relevant risk indexes is calculated, weighted with the normalized weighting factor and taken as basis for the next calculation. • Increment: The risk index of table column (target) is incremented by a fixed value. This value is specified in Weighting/Change value. • Decrement: The risk index of the table column (target) is decreased by a fixed value. This value is specified in Weighting/Change value. • Average (weighted): The average of all relevant risk indexes is calculated, weighted, and taken as basis for the next calculation. • Average (normalized): The average of all relevant risk indexes is calculated with the normalized weighting factor and taken as basis for the next calculation. • Reduction: Used when calculating the reduced risk index for compliance rules, SAP functions, company policies, and attestation policies. You cannot add custom functions with this calculation type!
Weighting/change value	Use the slider to set the value either with which to weight the risk index in the overall calculation or the value by which the risk index will change.

4. Click **Save**.

Disabling/enabling risk index functions

If risk index functions are **not** to be taken into account in the overall calculation of risk indexes, you can disable them. You can enable disabled risk index functions again.

To disable an enabled risk index function

1. In the menu bar, click **Setup > Risk index functions**.
2. On the **Risk Index Functions** page, click the risk index function you want to disable.
3. In the **Edit Risk Index Function** pane, select the **Disable** check box.
4. Click **Save**.

To enable a disabled risk index function

1. In the menu bar, click **Setup > Risk index functions**.
2. On the **Risk Index Functions** page, click the risk index function you want to enable.
3. In the **Edit Risk Index Function** pane, clear the **Disable** check box.
4. Click **Save**.

Starting risk index calculation manually

The risk index calculation is automatically started by the following events:

- A risk index function was modified.
- Objects in the source table have changed.
- A scheduled calculation task is being run.

You can also trigger the risk index calculation manually. This allows changes that do not trigger automatic risk index calculation to be applied to calculated risk indexes. For example, this is required to take into account approval of attestation cases in calculated risk indexes. Similarly, risk index function without source tables assigned to them are only taken into account during a cyclical recalculation.

To start manual risk index calculation

1. In the menu bar, click **Setup > Risk index functions**.
2. On the **Risk Index Functions** page, click **Recalculate risk index**.

Based on the risk index history, resulting risk indexes are calculated for employees, user accounts, and hierarchical roles. All direct and indirectly assigned objects are taken into account.

Responsibilities

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

Detailed information about this topic

- [My responsibilities](#) on page 168
- [Managing task delegations](#) on page 303
- [Ownerships](#) on page 306

My responsibilities

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

- Identities
- 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](#)

Detailed information about this topic

- [Managing my departments](#) on page 169
- [Managing my application roles](#) on page 184
- [Managing my business roles](#) on page 199
- [Managing my identities](#) on page 214
- [Managing my cost centers](#) on page 234
- [Managing my multi-request resources](#) on page 248
- [Managing my multi requestable/unsubscribable resources](#) on page 250
- [Managing my resources](#) on page 252
- [Managing my locations](#) on page 263
- [Managing my system entitlements](#) on page 277
- [Managing my system roles](#) on page 292
- [Managing my assignment resources](#) on page 301

Managing my departments

You can perform a variety of actions on the departments that you manage and gather information about them.

Detailed information about this topic

- [Displaying my departments](#) on page 170
- [Creating your own departments](#) on page 170
- [Displaying and editing my department main data](#) on page 171
- [Copying/splitting my departments](#) on page 173
- [Comparing and merging my departments](#) on page 175
- [Restoring my departments to their previous state](#) on page 176
- [Managing my department memberships](#) on page 176
- [Managing my departments' entitlements](#) on page 180
- [Displaying my departments' rule violations](#) on page 181
- [My departments' history](#) on page 182
- [Restoring my deleted departments](#) on page 183

Displaying my departments

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

To display departments

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Departments**.
This opens the **Departments** page and displays all the departments for which you are responsible.
3. (Optional) To display details of a department, click the department.

Creating your own departments

You can create new departments for which you are responsible.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a department

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Departments**.
3. On the **Departments** page click **+ Create department**.
4. In the **Create Department** pane, enter the main data of the department in the respective fields.

You can edit the following main data.

Table 27: Department main data

Property	Description
Department	Enter a full, descriptive name for the department.
Short name	Enter a short name for the department.
Object ID	Enter a unique object ID for the department. For example, the object ID is required in SAP systems for assigning identities to departments.
Parent department	Click Select/Change and select a department to be the parent department for organizing the department hierarchically. If you want the department at the root of a department hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the department.
Deputy manager	Select an identity to act as a deputy to the department's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Location	Click Select/Change and select the location the department is primarily assigned to.
Attestors	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the department.
Cost center	Click Select/Change and select the cost center the department is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the department.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the department.
Description	Enter a description for the department.

5. Click **Create**.

Displaying and editing my department main data

You can display and edit the main data of the departments for which you are responsible.

To display and edit a department's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesDepartments**.
3. On the **Identities** page, click the department whose main data you want to display/edit.
4. In the **Edit Department** pane.

You can edit the following main data.

Table 28: Department main data

Property	Description
Department	Enter a full, descriptive name for the department.
Short name	Enter a short name for the department.
Object ID	Enter a unique object ID for the department. For example, the object ID is required in SAP systems for assigning identities to departments.
Parent department	Click Select/Change and select a department to be the parent department for organizing the department hierarchically. If you want the department at the root of a department hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the department.
Deputy manager	Select an identity to act as a deputy to the department's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Location	Click Select/Change and select the location the department is primarily assigned to.
Attestors	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the department.
Cost center	Click Select/Change and select the cost center the department is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the department.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the department.
Description	Enter a description for the department.

5. Click **Save**.

Copying/splitting my departments

You can copy or move memberships and entitlements from departments you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a department or move memberships and entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Departments**.
3. On the **Departments** page click the department you want to copy or whose memberships and entitlements you want to move.
4. In the **Edit Department** pane, click **⋮ (Actions) > Split**.
5. In the **Split** pane, in the **Type of new object** menu, select which type to give the new object.
6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

TIP: After the object has been created, you can add the remaining main data (see [Displaying and editing my department main data](#) on page 171, [Displaying and editing my business roles' main data](#) on page 202, [Displaying and editing my cost center main data](#) on page 236, or [Displaying and editing my locations' main data](#) on page 265).

7. Click **Next**.
8. In the **Select assignments to be copied or moved to the new object** step, perform the following actions:
 - To neither copy nor move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and do not copy or move to new object**. The entitlement/membership is later only available in the source object.
 - To copy or move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new object**. The entitlement/membership is included later in the source object as well as the target object.
 - To move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new object**. The entitlement/membership is later removed from the source object and only included in the target object.
9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.

Related topics

- [Managing my department memberships](#) on page 176
- [Managing my departments' entitlements](#) on page 180

Comparing and merging my departments

You can compare properties of departments that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a department

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Departments**.
3. On the **Departments** page, click the department you want to compare and merge.
4. In the **Edit Department** pane, click **⋮ (Actions) > Compare and merge**.
5. In the **Compare and Merge** pane, in the **Comparison object** field, click **Select**.
6. In the **Edit Property** pane, in the **Object type** menu, select whether you want to compare and merge the department with a business role, department, cost center, or location.
7. Click the relevant business role, department, cost center, or location.
8. Click **Next**.

The assigned memberships and entitlements of both objects are listed with the following information in the **View comparison result** step.

Table 29: Overview of the assignments

Column	Description
Assigned object	Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.
This object	Shows you the assignment type of the entitlement/membership in the source or comparison object. The following assignment types are available. <ul style="list-style-type: none">• Direct• Inherited• Requested• Dynamic• Not assigned
Comparison object	For more detailed information about assigning company resources, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i> .

9. Click **Next**.

10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Merge**.

Related topics

- [Managing my department memberships](#) on page 176
- [Managing my departments' entitlements](#) on page 180

Restoring my departments to their previous state

You can compare the current status of a department that you are responsible for to its status at another time and completely or partially restore the historical state.

To restore a department to a previous state

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Departments**.
3. On the **Departments** page, click the department you want to roll back.
4. In the **Edit Department** pane, click **⋮ (Actions) > Reset to previous state**.
5. In the **Reset to Previous State** pane, in the **Comparison date** field, specify a date.
6. Click **Next**.

The **View comparison result** step shows all changes that have taken place since the given date.

7. Select the check box next to the property that you want to restore to its previous state.
8. Click **Next**.
9. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
10. Click **Next**.

Related topics

- [Managing my department memberships](#) on page 176
- [Managing my departments' entitlements](#) on page 180

Managing my department memberships

As soon as an identity is assigned to a department, the identity becomes a member in the department.

Detailed information about this topic

- [Displaying memberships in my departments](#) on page 177
- [Analyzing assignments to my departments](#) on page 177
- [Adding identities to my departments](#) on page 177
- [Removing identities from my departments](#) on page 179

Displaying memberships in my departments

You can display identities that are assigned departments for which you are responsible.

To display identities that are assigned a department

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Departments**.
3. On the **Departments** page, click the department whose memberships you want to display.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To display all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my departments

You can display how a department assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Departments**.
3. On the **Departments** page, click the department whose memberships you want to display.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click the membership to display its assignment analysis.

Adding identities to my departments

You can assign identities to departments for which you are responsible.

The following assignment options are available:

- Assignment by [request](#)
- Automatic assignment through a [dynamic role](#)
- Revoking [exclusion](#) of a member

To assign an identity to a department using a request

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Departments**.
3. On the **Departments** page, click the department to which you want to add an identity.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click **Request memberships**.
7. In the **Request Memberships** pane, next to the identity to which you want to assign the department, select the check box.
8. Click **Request memberships**.
9. Close the **Edit Department** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

Once the request has been granted approval, the identity is assigned to the department.

To add members automatically through a dynamic role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Departments**.
3. On the **Departments** page, click the department for which you want to create a dynamic role.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Automatic memberships**.
6. Click **Create dynamic role**.
7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:
 - a. Click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition, click **Add another condition** and repeat the steps.

- f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

TIP: To remove a condition, click  (**Delete**).

For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.

8. Click **Save**.
9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.
10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.
11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Departments**.
3. On the **Departments** page, click the department to which you want to re-add a member.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.
6. Select the check box next to the identity you want to add again as a member.
7. Click **Remove exclusion**.

Related topics

- [Requesting products](#) on page 71

Removing identities from my departments

You can remove departments from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a department from an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Departments**.
3. On the **Departments** page, click the department that has a membership you want to delete.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.

6. Next to the membership you want to delete, select the check box.
 7. Click **Remove**.
 8. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
 9. Click **Remove memberships**.
- TIP:** If you only selected direct memberships, confirm the prompt in the **Remove Membership** dialog with **Yes**.

Managing my departments' entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to system roles you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the departments.

Detailed information about this topic

- [Displaying my department entitlements](#) on page 180
- [Adding entitlements to my departments](#) on page 180
- [Deleting my department entitlements](#) on page 181

Displaying my department entitlements

You can display entitlements that are assigned departments for which you are responsible.

To display entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities** **Departments**.
3. On the **Departments** page, click the department whose entitlements you want to display.
4. In the **Edit Department** pane, click the **Permissions** tab.

Adding entitlements to my departments

You can add entitlements to departments for which you are responsible. You do this through requests.

To add an entitlement to a department

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Departments**.
3. On the **Departments** page, click the department to which you want to add an entitlement.
4. In the **Edit Department** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.
9. Close the **Edit Department** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

After the request has been granted approval, the entitlement is added to the department.

Related topics

- [Requesting products](#) on page 71

Deleting my department entitlements

You can delete entitlements that are assigned departments for which you are responsible.

To delete an entitlement of a department

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Departments**.
3. On the **Departments** page, click the department whose entitlements you want to delete.
4. In the **Edit Department** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying my departments' rule violations

You can display the rule violations of departments for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Departments**.
3. On the **Departments** page, click the department whose rule violations you want to display.
4. On the **Edit Department** pane, click the **Rule Violations** tab.

My departments' history

The Web Portal allows you to display historical data of departments for which you are responsible.

To do this, you have the following options:

Table 30: Historical data

View	Description
Events	Shows all events relating to the department in table form (see Displaying my department history on page 182).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my departments on page 183).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my departments on page 183).

Displaying my department history

To track changes, you can display the history of departments for which you are responsible.

To display the history

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Departments**.
3. On the **Departments** page, click the department whose history you want to display.
4. In the **Edit Department** pane, click the **History** tab.

Displaying the status overview of my departments

You can display all the changes effecting departments for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesDepartments**.
3. On the **Departments** page, click the department whose status overview you want to display.
4. In the **Edit Department** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of my departments

You can compare the current status of a department that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesDepartments**.
3. On the **Departments** page, click the department whose status you want to compare.
4. In the **Edit Department** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Restoring my deleted departments

You can restore deleted departments for which you were responsible. For example, a department can be deleted if two roles are merged (see [Comparing and merging my departments](#) on page 175).

To restore a deleted department

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesDepartments**.
3. On the **Departments** page, click **Restore deleted object**.
4. In the **Restore Deleted Object** pane, click the department that you want to restore.

5. Click **Next**.
6. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
7. Click **Next**.

Managing my application roles

Use application roles to quickly and simply assign entitlement profiles to identities that match their tasks and functions. One Identity Manager already supplies a number of default application roles.

You can perform a variety of actions on the application roles that you manage and gather information about them.

Detailed information about this topic

- [Displaying my application roles](#) on page 184
- [Creating your own application roles](#) on page 184
- [Displaying and editing my application roles' main data](#) on page 186
- [Restoring my application roles to their previous state](#) on page 187
- [Managing my application role memberships](#) on page 188
- [Displaying my application roles' rule violations](#) on page 192
- [My application roles' history](#) on page 192

Displaying my application roles

You can display all the application roles for which you are responsible.

To display application roles

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Application roles**.
This opens the **Application Roles** page and displays all the application roles for which you are responsible.
3. (Optional) To display details of an application role, click the application role.

Creating your own application roles

You can create new application roles for which you are responsible.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create an application role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Application roles**.
3. On the **Application Roles** page, click **+ Create application role**.
4. In the **Create Application Role** pane, enter the main data of the application role in the respective fields.

You can edit the following main data.

Table 31: Main data of application roles

Property	Description
Application role	Enter a full, descriptive name for the application role.
Internal name	Enter a company internal name for the application role.
Parent application role	Click Select/Change and select an application role to be the parent application role to organize the application role hierarchically. If you want the application role at the root of an application role hierarchy, leave the field empty.
Manager	Click Select/Change and select the manager responsible for the application role.
Deputy manager	Click Select/Change and select an identity to act as a deputy to the application role's manager.
Description	Enter a description for the application role.
Comment	Enter a comment for the application role.
Full name	Shows the full name of the application role, which is automatically made up of the identifiers of the application role and the parent application role.
Department	Click Select/Change and select the department the application role is primarily assigned to.
Location	Click Select/Change and select the location the application role is primarily assigned to.
Cost center	Click Select/Change and select the cost center the application role is primarily assigned to.

5. Click **Create**.

Displaying and editing my application roles' main data

You can display and edit the main data of the application roles that you are responsible for.

To display and edit an application role's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesApplication roles**.
3. On the **Application Roles** page, click the application roles whose main data you want to display/edit.
4. In the **Edit Application role** pane.

You can edit the following main data.

Table 32: Main data of application roles

Property	Description
Application role	Enter a full, descriptive name for the application role.
Internal name	Enter a company internal name for the application role.
Parent application role	Click Select/Change and select an application role to be the parent application role to organize the application role hierarchically. If you want the application role at the root of an application role hierarchy, leave the field empty.
Manager	Click Select/Change and select the manager responsible for the application role.
Deputy manager	Click Select/Change and select an identity to act as a deputy to the application role's manager.
Description	Enter a description for the application role.
Comment	Enter a comment for the application role.
Full name	Shows the full name of the application role, which is automatically made up of the identifiers of the application role and the parent application role.
Department	Click Select/Change and select the department the application role is primarily assigned to.
Location	Click Select/Change and select the location the application role is primarily assigned to.
Cost center	Click Select/Change and select the cost center the application role is primarily assigned to.

5. Click **Save**.

Restoring my application roles to their previous state

You can compare the current status of an application role that you are responsible for, to its status at another time and completely or partially restore the historical state.

To restore an application role to a previous state

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesApplication roles**.
3. On the **Application Roles** page, click the application role you want to roll back.
4. In the **Edit application role** pane, click **⋮ (Actions) > Reset to previous state**.
5. In the **Reset to Previous State** pane, in the **Comparison date** field, specify a date.
6. Click **Next**.
The **View comparison result** step shows all changes that have taken place since the given date.
7. Select the check box next to the property that you want to restore to its previous state.
8. Click **Next**.
9. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
10. Click **Next**.

Related topics

- [Managing my application role memberships](#) on page 188

Managing my application role memberships

As soon as an identity is assigned to an application role, the identity becomes a member in the application role.

Detailed information about this topic

- [Displaying memberships in my application roles](#) on page 188
- [Analyzing assignments to my application roles](#) on page 189
- [Assigning identities to my application roles](#) on page 189
- [Removing identities from my application roles](#) on page 191

Displaying memberships in my application roles

You can display identities that are assigned application roles for which you are responsible.

To display identities that are assigned an application role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Application roles**.
3. On the **Application Roles** page, click the application role whose memberships you want to display.
4. In the **Edit Application role** pane, click the **Memberships** tab.
5. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my application roles

You can display how an application role assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Application roles**.
3. On the **Application Roles** page, click the application role whose memberships you want to display.
4. In the **Edit Application role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click the membership to display its assignment analysis.

Assigning identities to my application roles

You can assign identities to application roles for which you are responsible.

The following assignment options are available:

- Assignment by [request](#)
- Automatic assignment through a [dynamic role](#)
- Revoking [exclusion](#) of a member

To assign an identity to a application role using a request

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Application roles**.
3. On the **Application Roles** page, click the application role to which you want to assign an identity.
4. In the **Edit Application Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Request memberships**.

6. In the **Request Memberships** pane, next to the identity to which you want to assign the application role, select the check box.
7. Click **Request memberships**.
8. Close the **Edit Application Role** pane.
9. In the menu bar, click **Requests > Shopping cart**.
10. On the **Shopping Cart** page, click **Submit**.
Once the request has been granted approval, the identity is assigned to the application role.

To add members automatically through a dynamic role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Application roles**.
3. On the **Application Roles** page, click the application role for which you want to create a dynamic role.
4. In the **Edit Application Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Automatic memberships**.
6. Click **Create dynamic role**.
7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:
 - a. Click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition, click **Add another condition** and repeat the steps.
 - f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

TIP: To remove a condition, click  (**Delete**).

For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.

8. Click **Save**.
9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.
10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.
11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Application roles**.
3. On the **Application Roles** page, click the application role to which you want to re-add a member.
4. In the **Edit Application Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.
6. Select the check box next to the identity you want to add again as a member.
7. Click **Remove exclusion**.

Related topics

- [Requesting products](#) on page 71

Removing identities from my application roles

You can remove application roles from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove an application role from an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Application roles**.
3. On the **Application Roles** page, click the application role that has a membership you want to delete.
4. In the **Edit Application Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.
6. Next to the membership you want to delete, select the check box.
7. Click **Remove**.
8. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
9. Click **Remove memberships**.

TIP: If you only selected direct memberships, confirm the prompt in the **Remove Membership** dialog with **Yes**.

Displaying my application roles' rule violations

You can display the rule violations of application roles for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesApplication roles**.
3. On the **Application Roles** page, click the application role whose rule violations you want to display.
4. On the **Edit Application Role** pane, click the **Rule Violations** tab.

My application roles' history

The Web Portal allows you to display historical data of application roles for which you are responsible.

To do this, you have the following options:

Table 33: Historical data

View	Description
Events	Shows all events relating to the application role in table form (see Displaying my application roles' history on page 192).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my application roles on page 193).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my application roles on page 193).

Displaying my application roles' history

To track changes, you can display the history of application roles for which you are responsible.

To display the history

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesApplication roles**.

3. On the **Application Roles** page, click the application role whose history you want to display.
4. In the **Edit Application role** pane, click the **History** tab.

Displaying the status overview of my application roles

You can display all the changes effecting application roles for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Application roles**.
3. On the **Application Roles** page, click the application role whose status overview you want to display.
4. In the **Edit Application role** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of my application roles

You can compare the current status of an application role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Application roles**.
3. On the **Application Roles** page, click the application role whose status you want to compare.
4. In the **Edit Application role** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Managing my devices

You can perform a variety of actions on devices that you manage and gather information about them.

Detailed information about this topic

- [Displaying my devices](#) on page 194
- [Creating your own devices](#) on page 194
- [Displaying and editing my devices' main data](#) on page 196
- [Deleting your own devices](#) on page 199

Displaying my devices

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

To display devices

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Devices**.
This opens the **Devices** page and displays all the devices for which you are responsible.
3. (Optional) To display details of a device, click the device.

Creating your own devices

You can create new devices for which you are responsible.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a device

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Devices**.
3. On the **Devices** page, click **+ Create device**.
4. In the **Create Device** pane, enter the device's main data in the respective fields.

You can edit the following main data.

Table 34: Mobile phone main data

Property	Description
Used by	Select the identity for the device to use.
Device model	Select the device model.
Manufacturer	Select the device manufacturer.

Property	Description
Device ID	Enter a name for the device.
Device status	Select the device status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
RAM [MB]	Enter the device's storage capacity (in megabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.

Table 35: PC main data

Property	Description
Used by	Select the identity for the device to use.
Device model	Select the model of the device.
Manufacturer	Select the device manufacturer.
Device ID	Enter a name for the device.
Device status	Select the device status.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
RAM [MB]	Enter the device's storage capacity (in megabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
MAC address	Enter the device's MAC address.
PC	Select the check box if this is a simple desktop PC for an

Property	Description
	identity.
Servers	Select the check box if this is a server.
VM Host	Select the check box if this is a host for a virtual machine.
VM Client	Select the check box if this is a virtual machine.
VM Host	Select the device on which the virtual machine is installed. The select is available if the VM Client check box is set.

Table 36: Tablet main data

Property	Description
Used by	Select the identity for the device to use.
Device model	Select the model of the device.
Manufacturer	Select the device manufacturer.
Device ID	Enter a name for the device.
Device status	Select the device status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
RAM [MB]	Enter the device's storage capacity (in megabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.

5. Click **Create**.

Displaying and editing my devices' main data

You can display and edit the main data of the devices for which you are responsible.

To display and edit a device's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Devices**.
3. On the **Devices** page, click the devices whose main data you want to display/edit.
4. In the **Edit Device** pane.

You can edit the following main data.

Table 37: Mobile phone main data

Property	Description
Used by	Select the identity for the device to use.
Device model	Select the device model.
Manufacturer	Select the device manufacturer.
Device ID	Enter a name for the device.
Device status	Select the device status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
RAM [MB]	Enter the device's storage capacity (in megabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.

Table 38: PC main data

Property	Description
Used by	Select the identity for the device to use.
Device model	Select the model of the device.
Manufacturer	Select the device manufacturer.
Device ID	Enter a name for the device.

Property	Description
Device status	Select the device status.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
RAM [MB]	Enter the device's storage capacity (in megabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.
MAC address	Enter the device's MAC address.
PC	Select the check box if this is a simple desktop PC for an identity.
Servers	Select the check box if this is a server.
VM Host	Select the check box if this is a host for a virtual machine.
VM Client	Select the check box if this is a virtual machine.
VM Host	Select the device on which the virtual machine is installed. The select is available if the VM Client check box is set.

Table 39: Tablet main data

Property	Description
Used by	Select the identity for the device to use.
Device model	Select the model of the device.
Manufacturer	Select the device manufacturer.
Device ID	Enter a name for the device.
Device status	Select the device status.
Phone	Enter the device's telephone number.
Location description	Enter additional information about the device's location.
Serial number	Enter the device's serial number.
RAM [MB]	Enter the device's storage capacity (in megabytes).
Operating system	Enter the name of the device's operating system.
Operating system version	Enter the version number of the device's operating system.

Property	Description
Carrier	Enter the name of the device's carrier.
IMEI	Enter the device's IMEI (unique identification number).
ICCID	Enter the IMEI (unique identification number) of the device's SIM card.
MAC address	Enter the device's MAC address.

5. Click **Save**.

Deleting your own devices

You can delete device for which you are responsible.

To delete a device

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Devices**.
3. On the **Device** page, click the device you want to delete.
4. In the **Edit Device** pane, click  **Delete device**.
5. In the **Delete Device** dialog, confirm the prompt with **Yes**.

Managing my business roles

Business roles are defined based on resources to perform specific functions.

Business roles are objects for mapping company-specific functions in One Identity Manager. Business roles map company structures with similar functionality that exist in addition to departments, cost centers, and locations. This might be projects groups, for example.

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

Detailed information about this topic

- [Displaying my business roles](#) on page 200
- [Creating your own business roles](#) on page 200
- [Displaying and editing my business roles' main data](#) on page 202
- [Copying/splitting my business roles](#) on page 204
- [Comparing and merging my business roles](#) on page 205

- [Restoring my business roles to their previous state](#) on page 206
- [Managing my business role memberships](#) on page 207
- [Managing my business roles' entitlements](#) on page 210
- [Displaying my business roles' rule violations](#) on page 212
- [My business roles' history](#) on page 212
- [Restoring my deleted business roles](#) on page 214

Displaying my business roles

You can display all the business roles for which you are responsible.

To display business roles

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Business roles**.
This opens the **Business Roles** page and display all the business roles for which you are responsible.
3. (Optional) To display details of a business role, click the business role.

Creating your own business roles

You can create new business roles for which you are responsible.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a business role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Business roles**.
3. On the **Business Roles** page, click **+ Create business role**.
4. In the **Create Business Role** pane, enter the main data of the business role in the respective fields.

You can edit the following main data.

Table 40: Business role main data

Property	Description
Business role	Enter a full, descriptive name for the business role.
Short name	Enter a short name for the business role.
Internal name	Enter a company internal name for the business role.
Description	Enter a description for the business role.
Role class	When you create the business role: Select the role class of the business role. To differentiate between different business roles, define company specific role classes. Role classes are used to specify which company resource assignments are possible through roles in a role class.
Parent business role	Click Select/Change and select a business role to be the parent business role for organizing the business role hierarchically. If you want the business role at the root of a business role hierarchy, leave the field empty.
Role type	Select the role type of the business role. Role types are mainly used to regulate approval policy inheritance.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the business role.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the business role.
Manager	Select the manager who is responsible for the business role.
Deputy manager	Select an identity to act as a deputy to the business role's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Identities do not inherit	Select this check box if you want to temporarily prevent identities from inheriting this business role.
Comment	Enter a comment for the business role.

5. Click **Create**.

Displaying and editing my business roles' main data

You can display and edit the main data of the business roles for which you are responsible.

To display and edit a business role's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Business roles**.
3. On the **Business Roles** page, click the business role whose main data you want to display/edit.
4. In the **Edit Business Role** pane.

You can edit the following main data.

Table 41: Business role main data

Property	Description
Business role	Enter a full, descriptive name for the business role.
Short name	Enter a short name for the business role.
Internal name	Enter a company internal name for the business role.
Description	Enter a description for the business role.
Role class	When you create the business role: Select the role class of the business role. To differentiate between different business roles, define company specific role classes. Role classes are used to specify which company resource assignments are possible through roles in a role class.
Parent business role	Click Select/Change and select a business role to be the parent business role for organizing the business role hierarchically. If you want the business role at the root of a business role hierarchy, leave the field empty.
Role type	Select the role type of the business role. Role types are mainly used to regulate approval policy inheritance.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the business role.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the business role.
Manager	Select the manager who is responsible for the business role.
Deputy manager	Select an identity to act as a deputy to the business role's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Identities do not inherit	Select this check box if you want to temporarily prevent identities from inheriting this business role.
Comment	Enter a comment for the business role.

5. Click **Save**.

Copying/splitting my business roles

You can copy or move memberships and entitlements from business roles you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a business role or move memberships and entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business Roles** page, click the business role you want to copy or whose memberships and entitlements you want to move.
4. In the **Edit Business Role** pane, click **⋮ (Actions) > Split**.
5. In the **Split** pane, in the **Type of new object** menu, select which type to give the new object.
6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

TIP: After the object has been created, you can add the remaining main data (see [Displaying and editing my department main data](#) on page 171, [Displaying and editing my business roles' main data](#) on page 202, [Displaying and editing my cost center main data](#) on page 236, or [Displaying and editing my locations' main data](#) on page 265).
7. Click **Next**.
8. In the **Select assignments to be copied or moved to the new object** step, perform the following actions:
 - To neither copy nor move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and do not copy or move to new object**. The entitlement/membership is later only available in the source object.
 - To copy or move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new object**. The entitlement/membership is included later in the source object as well as the target object.
 - To move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new object**. The entitlement/membership is later removed from the source object and only included in the target object.
9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.

Related topics

- [Managing my business role memberships](#) on page 207
- [Managing my business roles' entitlements](#) on page 210

Comparing and merging my business roles

You can compare properties of business roles that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a business role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business roles** page, click the business role that you want to compare and merge.
4. In the **Edit Business Role** pane, click **⋮ (Actions) > Compare and merge**.
5. In the **Compare and Merge** pane, in the **Comparison object** field, click **Select**.
6. In the **Edit Property** pane, in the **Object type** menu, select whether you want to compare and merge the business role with a business role, department, cost center, or location.
7. Click the relevant business role, department, cost center, or location.
8. Click **Next**.

The assigned memberships and entitlements of both objects are listed with the following information in the **View comparison result** step.

Table 42: Overview of the assignments

Column	Description
Assigned object	Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.

Column	Description
This object	<p>Shows you the assignment type of the entitlement/membership in the source or comparison object. The following assignment types are available.</p> <ul style="list-style-type: none"> • Direct • Inherited • Requested • Dynamic • Not assigned <p>For more detailed information about assigning company resources, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p>
Comparison object	

9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Merge**.

Related topics

- [Managing my business role memberships](#) on page 207
- [Managing my business roles' entitlements](#) on page 210

Restoring my business roles to their previous state

You can compare the current status of a business role that you are responsible for, to its status at another time and completely or partially restore the historical state.

To restore a business role to a previous state

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business Roles** page, click the business role you want to roll back.
4. In the **Edit Business Role** pane, click **(Actions) > Reset to previous state**.
5. In the **Reset to Previous State** pane, in the **Comparison date** field, specify a date.
6. Click **Next**.

The **View comparison result** step shows all changes that have taken place since the given date.

7. Select the check box next to the property that you want to restore to its previous state.
8. Click **Next**.
9. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
10. Click **Next**.

Related topics

- [Managing my business role memberships](#) on page 207
- [Managing my business roles' entitlements](#) on page 210

Managing my business role memberships

As soon as a business role is assigned to an identity, the identity becomes a member in the business role.

Detailed information about this topic

- [Displaying my business roles' memberships](#) on page 207
- [Analyzing assignments to my business roles](#) on page 208
- [Assigning identities to my business roles](#) on page 208
- [Removing identities from my business roles](#) on page 210

Displaying my business roles' memberships

You can display identities that are assigned business roles for which you are responsible.

To display identities that are assigned a business role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business Roles** page, click the business role whose memberships you want to display.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To display all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my business roles

You can display how a business role under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business Roles** page, click the business role whose memberships you want to display.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click the membership to display its assignment analysis.

Assigning identities to my business roles

You can assign identities to business roles for which you are responsible.

The following assignment options are available:

- Assignment by [request](#)
- Automatic assignment through a [dynamic role](#)
- Revoking [exclusion](#) of a member

To assign an identity to a business role using a request

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business roles** page, click the business role to which you want to assign an identity.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click **Request memberships**.
7. In the **Request Memberships** pane, next to the identity to which you want to assign the business role, select the check box.
8. Click **Request memberships**.
9. Close the **Edit Business Role** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

Once the request has been granted approval, the identity is assigned to the business role.

To add members automatically through a dynamic role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
 2. In the navigation, click Identities **Business roles**.
 3. On the **Business Roles** page, click the business role for which you want to create a dynamic role.
 4. In the **Edit Business Role** pane, click the **Memberships** tab.
 5. On the **Memberships** tab, click **Automatic memberships**.
 6. Click **Create dynamic role**.
 7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:
 - a. Click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition, click **Add another condition** and repeat the steps.
 - f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.
- TIP:** To remove a condition, click  (**Delete**).
- For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.
8. Click **Save**.
 9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.
 10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.
 11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities **Business roles**.
3. On the **Business Roles** page, click the business role to which you want to re-add a member.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.
7. Click **Remove exclusion**.

Related topics

- [Requesting products](#) on page 71

Removing identities from my business roles

You can remove business roles from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a business role from an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Business roles**.
3. On the **Business Roles** page, click the business role with a membership you want to delete.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.
6. Next to the membership you want to delete, select the check box.
7. Click **Remove**.
8. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
9. Click **Remove memberships**.

TIP: If you only selected direct memberships, confirm the prompt in the **Remove Membership** dialog with **Yes**.

Managing my business roles' entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. Assigning identities to business roles avoids you having to assign entitlements separately to each identity. All a business role's entitlements are automatically assigned to all the identities assigned to the business role.

Detailed information about this topic

- [Displaying my business roles' entitlements](#) on page 211
- [Adding entitlements to my business roles](#) on page 211
- [Deleting my business roles' entitlements](#) on page 212

Displaying my business roles' entitlements

You can display entitlements that are assigned business roles for which you are responsible.

To display entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Business roles**.
3. On the **Business Roles** page, click the business role whose entitlements you want to display.
4. In the **Edit Business Role** pane, click the **Permissions** tab.

Adding entitlements to my business roles

You can add entitlements to business roles for which you are responsible. You do this through requests.

To add an entitlement to a business role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Business roles**.
3. On the **Business Roles** page, click the business role to which you want to add an entitlement.
4. In the **Edit Business Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.
9. Close the **Edit Business Role** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

After the request has been granted approval, the entitlement is added to the business role.

Related topics

- [Requesting products](#) on page 71

Deleting my business roles' entitlements

You can delete entitlements that are assigned business roles for which you are responsible.

To delete an entitlement of a business role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities **Business roles**.
3. On the **Business Roles** page, click the business role whose entitlements you want to delete.
4. In the **Edit Business Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying my business roles' rule violations

You can display the rule violations of business roles for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities **Business roles**.
3. On the **Business Roles** page, click the business role whose rule violations you want to display.
4. On the **Edit Business Role** pane, click the **Rule Violations** tab.

My business roles' history

The Web Portal allows you to display historical data of business roles for which you are responsible.

To do this, you have the following options:

Table 43: Historical data

View	Description
Events	Shows all events relating to the business role in table form (see Displaying my business roles' history on page 213).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my business roles on page 213).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my business roles on page 214).

Displaying my business roles' history

To track changes, you can display the history of business roles for which you are responsible.

To display the history

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business Roles** page, click the business role whose history you want to display.
4. In the **Edit Business Role** pane, click the **History** tab.

Displaying the status overview of my business roles

You can display all the changes effecting business roles for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business Roles** page, click the business role whose status overview you want to display.
4. In the **Edit Business Role** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of my business roles

You can compare the current status of a business role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business Roles** page, click the business role whose status you want to compare.
4. In the **Edit Business Role** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Restoring my deleted business roles

You can restore deleted business roles for which you were responsible. For example, a business role can be deleted if two roles are merged (see [Comparing and merging my business roles](#) on page 205).

To restore a deleted business role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesBusiness roles**.
3. On the **Business roles** page, click **Restore deleted object**.
4. In the **Restore Deleted Object** pane, click the business role that you want to restore.
5. Click **Next**.
6. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
7. Click **Next**.

Managing my identities

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

Detailed information about this topic

- [Displaying my identities](#) on page 215
- [Creating your own identities](#) on page 216
- [Comparing my identities](#) on page 219
- [Displaying and editing my identities' main data](#) on page 220
- [Displaying my identities' risk indexes](#) on page 222
- [Deactivating my identities](#) on page 222
- [Reactivating my identities](#) on page 223
- [Marking my identities as security risks](#) on page 223
- [Revoking my identities' security risks](#) on page 223
- [Assigning other managers to my identities](#) on page 224
- [Creating passcodes for my identities](#) on page 225
- [Creating reports about my identities](#) on page 225
- [Managing my identities' memberships](#) on page 226
- [Displaying identities' organizational charts](#) on page 230
- [My identities' history](#) on page 230
- [Displaying my identity requests](#) on page 232
- [Managing my identities' attestation cases](#) on page 232
- [Displaying my identities' rule violations](#) on page 234

Displaying my identities

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

To display identities

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
This opens the **Identities** page and displays all the identities that report directly to you.
3. (Optional) To also display identities that report indirectly to you, deselect the **Identities you are directly responsible for** option.
4. (Optional) To display details of an identity, click the identity.

Creating your own identities

You can add new identities for which you are responsible. This function is mainly designed for adding external identities. For example, subcontractors who are not entered in the human resources department. Data from new identities 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.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click **+ Create identity**.
4. In the **Create identity** pane, enter the identity's main data in the respective fields.

You can edit the following main data.

Table 44: Identities main data

Property	Description
Unique data	
First name	Enter the identity's first name.
Last name	Enter the identity's last name.
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Personal data	
Second name	Enter the identity's middle name.
Date of birth	Enter the identity's date of birth. Click the  (Calendar) to do this and use the date picker to select the date of birth.
Personnel number	Enter the identity's personnel number.
Gender	In the menu, select the identity's gender.
Resetting the password through the help desk is permitted.	Select the check box to allow password help desk staff to reset the identity's password in the Operations Support Web Portal.

Organizational information

Property	Description
Primary cost center	Click Select/Change and select the identity's primary cost center.
Primary department	Click Select/Change and select the identity's primary department.
External	Select the check box if this is an external identity.
Identity	<p>Select the identity type of the identity:</p> <ul style="list-style-type: none"> • Primary identity: Default identity for an identity. The identity has a default user account. • Organizational identity: Virtual identity (sub identity) for mapping different roles of an identity within the organization. The sub identity is associated with a user account of the Organizational identity type. In addition, specify a main identity. • Personal administrator identity: Virtual identity (sub identity) associated with a user account of type Personal administrator identity type. In addition, specify a main identity. • Sponsored identity: Pseudo identity associated with a user account of type Sponsored identity. Also assign a manager to the identity. • Shared identity: Pseudo identity associated with an administrative user account of type Shared identity. Also assign a manager to the identity. • Service identity: Pseudo identity associated with a user account of type Service identity. Also assign a manager to the identity. • Machine identity: Pseudo identity for mapping machine identities. <p>For more information about mapping multiple identities of one identity, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p>
Employee type	In the menu, select what type of identity this is. For example, an identity of this company or a trainee.
Entry date	Enter the date the identity started at the company. Click the  (Calendar) and use the date picker to select the starting date.
Leaving date	Enter the date that the identity leaves the company. Click the

Property	Description
	 (Calendar) to do this and use the date picker to select the leaving date.
Manager	Shows you the identity's manager. TIP: If necessary, you can transfer the identity's manager at a later date (see Assigning other managers to my identities on page 224).
Permanently deactivated	Select the check box if you want the identity to be permanently deactivated (see Deactivating my identities on page 222).
Temporarily disabled	Select the check box to activate the identity at a later date then click the  (Calendar) and use the date picker to select the date to activate the identity.

Details of the location.

Primary location	Click Select/Change and select the identity's primary location.
Building	Enter the building where the identity works.
Floor	Enter which floor the identity works on.
Room	Enter the room the identity works in.
Street	Enter the street or road where the identity works.
Zip code	Enter the zip code of the identity's work location.
City	Enter the city where the identity works.
Country	In the menu, select the country where the identity works.
State	In the menu, select the state where the identity works.

The Web Portal checks whether identities with certain identical properties already exist.

- (Optional) Depending on the result of the check, you can display identities with identical properties and adjust the main data of the identities if necessary.

- Click **Create**.

Saving then checks again whether identities with certain identical properties already exist.

- (Optional) If the check finds an identity with identical properties, perform one of the following actions:

- To create the identity, in the **Create Identity with Same Properties** dialog, click **Yes**.

- To edit the identity and its properties before creating it, in the **Create Identity with Same Properties** dialog, click **No** and edit the main data of the identity you want to create.

Comparing my identities

You can compare identities that directly or indirectly report to you, with each other. For example, you can identify missing entitlements for individual identities so that they can be requested again in a targeted manner.

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities**.
3. On the **Identities** page, perform the following:
 - To compare identities that report directly to you, click **⋮ (Actions) > Compare identities who report directly to you**.
 - To compare identities that report directly and indirectly to you, click **⋮ (Actions) > Compare identities who report indirectly to you**.
4. In the **Specify Parameters** pane, perform the following actions:
 - a. In the **Identities to compare** field, click **Select**.
 - b. In the **Edit Property** pane, select the check boxes next to the identities you want to compare.
 - c. Click **Apply**.
5. (Optional) To specify how to mark the similarities, in the **Specify Parameters** pane, perform the following actions:
 - a. In the **Lower bound [%] yellow** field, specify the percentage of similarity required before properties are highlighted in yellow. For example, if you enter a value of **70** here, all the properties that have a similarity of 70% or more will be marked in orange.
 - b. In the **Lower bound [%] orange**, specify the percentage of similarity required before properties are highlighted in orange. For example, if you enter the value **50** here, then all properties that have a similarity of 50% or more will be marked in orange.
6. (Optional) To specify which object types to include in the comparison, perform the following actions:
 - a. In the **Select object types** field, click **Select**.
 - b. In the **Edit Property** pane, select the check boxes next to the object types you want to take into account.
 - c. Click **Apply**.
7. Click **Show report**.

Displaying and editing my identities' main data

You can display and edit the main data of the identities for which you are responsible.

To display and edit an identity's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click the identity whose main data you want to display/edit.
4. In the **Edit Identity** pane, expand the one of the sections.
5. Make your changes in the corresponding fields:

You can edit the following main data.

Table 45: Identities main data

Property	Description
Personal data	
Last name	Enter the identity's last name.
First name	Enter the identity's first name.
Middle name	Enter the identity's middle name.
Date of birth	Enter the identity's date of birth. Click the  (Calendar) to do this and use the date picker to select the date of birth.
Personnel number	Enter the identity's personnel number.
Gender	In the menu, select the identity's gender.
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Resetting the password through the help desk is permitted.	Select the check box to allow password help desk staff to reset the identity's password in the Operations Support Web Portal.
Identity does not pose a security risk/Identity poses a security risk	Toggle the switch to specify whether the identity poses a security risk or not (see Marking my identities as security risks on page 223).
Organizational information	
Primary cost center	Click Select/Change and select the identity's primary cost center.
Primary department	Click Select/Change and select the identity's primary department.
External	Select the check box if this is an external identity.
Employee type	In the menu, select what type of identity this is. For example, an identity of this company or a trainee.
Entry date	Enter the date the identity started at the company. Click the  (Calendar) and use the date picker to select the starting date.
Leaving date	Enter the date that the identity leaves the company. Click the  (Calendar) to do this and use the date picker to select the leaving date.

6. Click **Save**.

Displaying my identities' risk indexes

You can display identities' risk indexes that you are responsible for and analyze how they are put together.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display and analyze an identity's risk index

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the identity whose risk index you want to display and analyze.
4. In the **Edit Identity** pane, click **⋮ (Actions) > Analyze risk**.

Deactivating my identities

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

Effects of permanent deactivating an identity are:

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

To deactivate an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the identity you want to deactivate.
4. In the **Edit Identity** pane, expand the **Organizational information** section.
5. In the **Organizational Information** section, select the **Permanently deactivated** check box.
6. Click **Save**.

Reactivating my identities

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

To reactivate an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the identity you want to activate.
4. In the **Edit Identity** pane, expand the **Organizational information** section.
5. In the **Organizational Information** pane, clear the **Permanently deactivated** check box.
6. Click **Save**.

Marking my identities as security risks

You can mark identities that you manage as a security risk. Then the user accounts and resources of the affected identity are locked.

To mark an identity as a security risk

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the identity you want to mark as a security risk.
4. In the **Edit Identity** pane, toggle the switch next to **Identity poses a security risk**.
5. In the **Mark Identity as Security Risk** dialog, confirm the prompt with **Yes**.
The text next to the switch changes to **Identity poses a security risk**.
6. Click **Save**.

Related topics

- [Displaying and editing my identities' main data](#) on page 220

Revoking my identities' security risks

If identities that you manage have been marked as a security risk, you can unmark them again. Then the affected identity regains access to user accounts and resources.

To revoke an identity's security risk

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the relevant identity.
4. In the **Edit Identity** pane, toggle the switch next to **Identity poses a security risk**.
5. In the **Resolve Security Risk** dialog, confirm the prompt with **Yes**.
The text next to the switch changes to **Identity does not pose a security risk**.
6. Click **Save**.

Related topics

- [Displaying and editing my identities' main data](#) on page 220

Assigning other managers to my identities

You can assign other managers to the identities for which you are responsible.

To assign a new manager to an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlementsBusiness rolesSystem rolesDepartmentsCost centersLocationsApplication rolesResourcesAssignment resourcesMulti-request resourcesSoftwareMulti requestable/unsubscribable resourcesDevices**.
3. On the **Identities** page, click the identity that you want to assign to a new manager.
4. In the **Edit Identity Data** pane, click **Assign to new manager**.
5. On the **Shopping Cart** page, click **Edit** next to **Assign new manager**.
6. In the **New manager assignment** pane, in the **New manager** menu, select the manager you want to assign to the identity.
7. (Optional) If the identity for which you are selecting a new manager already has entitlements or products assigned, they are removed or unsubscribed by default on the effective date. If you want the identity to retain these entitlements or products when transferring to the new manager, clear the check boxes next to the respective entitlements and products.
8. (Optional) In the **Reason** field, enter why you are assigning a new manager.
9. (Optional) In the **Priority** menu, select the priority.
10. (Optional) To specify from when the new manager is responsible for the identity, enter the date in the **Valid from** field. If you leave the field blank, the change of manager will be carried out immediately after the new manager is approved.
11. Click **Save**.

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

NOTE: On the **Pending Requests** page, your request to change managers is presented to the new manager to be granted or denied approval (see [Approving new managers' pending requests](#) on page 96). After the new manager approves this requests, the new manager is assigned.

Related topics

- [Approving new managers' pending requests](#) on page 96

Creating passcodes for my identities

If identities, for which you are responsible, have forgotten their password for logging into the Web Portal and the passwords cannot be reset with the question and answer feature, you can create passcodes for them. With this passcode, identities can log on to the Password Reset Portal once and for a limited time.

To create a passcode for an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlementsBusiness rolesSystem rolesDepartmentsCost centersLocationsApplication rolesResourcesAssignment resourcesMulti-request resourcesSoftwareMulti requestable/unsubscribable resourcesDevices**.
3. On the **Identities** page, click the identity for which you want to create the passcode.
4. In the **Edit Identity Data** pane, click **Create passcode**.
The generated passcode and its validity are displayed in a dialog.
5. Note or copy the code and have it sent to the identity.

Creating reports about my identities

You can create the following reports on identities:

- [Reports](#) on individual identities
- [Reports](#) on a specific identity that reports directly to you
- [Reports](#) on all identities that report directly to you
- [Reports](#) on rule violations by identities that report directly to you.
- [Reports](#) on user accounts assigned to identities that report directly to you

To create a report on an individual identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click the identity for which you want to create a report.
4. In the **Edit Identity** pane, click **⋮ (Actions) > Download report**.

To create a report on identities that report to a specific identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click the identity to create a report on the identities who report directly to them.
4. In the **Edit Identity** section, click **⋮ (Actions) > Download report on identities who report directly to this identity**.

To create a report on all identities that report directly to you

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click **⋮ (Actions) > Download report on identities who report directly to you**.

To create a report on rule violations by identities that report directly to you

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click **⋮ (Actions) > Download report on rule violations by identities who report directly to you**.

To create a report on user accounts assigned to identities that report directly to you

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click **⋮ (Actions) > Download report on user accounts of identities who report directly to you**.

Managing my identities' memberships

Identity assignments to company structures and entitlements are enabled through membership in the respective company structures. For example, if an identity is going to be assigned to a particular department, it must first have membership in that department.

Detailed information about this topic

- [Analyzing my identities' membership assignments](#) on page 227
- [Displaying identities' departments](#) on page 354
- [Displaying identities' application roles](#) on page 354
- [Displaying identities' user accounts](#) on page 355
- [Displaying identities' business roles](#) on page 355
- [Displaying identities' cost centers](#) on page 355
- [Displaying identities' shops](#) on page 356
- [Displaying identities' locations](#) on page 356
- [Displaying identities' system entitlements](#) on page 356
- [Displaying identities' system roles](#) on page 357

Analyzing my identities' membership assignments

You can see how an identity membership under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click the identity whose memberships you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click the appropriate object types (for example, departments) in the navigation.
6. Click the membership to display its assignment analysis.

Displaying my identities' departments

You can display departments that are assigned identities for which you are responsible.

To display an identity's departments

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities**.
3. On the **Identities** page, click the identity whose departments you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Departments**.

Displaying my identities' application roles

You can display application roles that are assigned identities for which you are responsible.

To display an identity's application roles

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the identity whose application roles you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Application roles**.

Displaying my identities' user accounts

You can display user accounts that are assigned identities for which you are responsible.

To display an identity's user accounts

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the identity whose user accounts you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **User accounts**.

Displaying my identities' business roles

You can display business roles that are assigned identities for which you are responsible.

To display an identity's business roles

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the identity whose business roles you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Business roles**.

Displaying my identities' cost centers

You can display cost centers that are assigned identities for which you are responsible.

To display an identity's cost centers

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the identity whose cost centers you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Cost centers**.

Displaying my identities' shops

You can display shops that are assigned identities for which you are responsible.

To display an identity's shops

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities **System entitlements**.
3. On the **Identities** page, click the identity whose shops you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Shops**.

Displaying my identities' locations

You can display locations that are assigned identities for which you are responsible.

To display an identity's locations

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **Identities** page, click the identity whose locations you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Locations**.

Displaying my identities' system entitlements

You can display system entitlements that are assigned identities for which you are responsible.

To display an identity's system entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.

3. On the **Identities** page, click the identity whose system entitlements you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **System entitlements**.

Displaying my identities' system roles

You can display system roles that are assigned identities for which you are responsible.

To display an identity's system roles

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities**.
3. On the **Identities** page, click the identity whose system roles you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **System roles**.

Displaying identities' organizational charts

You can display the organizational charts of identities for which you are responsible.

To display an identity's organizational chart

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities**.
3. On the **Identities** page, click the identity whose organizational charts you want to display.
4. In the **Edit Identity** pane, click the **Organizational Chart** tab.

My identities' history

The Web Portal allows you to display historical data of identities for which you are responsible.

To do this, you have the following options:

Table 46: Historical data

View	Description
Events	Shows all events relating to the identity in table form (see Displaying my identities' history on page 231).

View	Description
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my identities on page 231).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my identities on page 231).

Displaying my identities' history

To track changes, you can display the history of identities for which you are responsible.

To display the history

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click the identity whose history you want to display.
4. In the **Edit Identity** pane, click the **History** tab.

Displaying the status overview of my identities

You can display all the changes effecting identities for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click the identity whose status overview you want to display.
4. In the **Edit Identity** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of my identities

You can compare the current status of an identity that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities **System entitlements**.
3. On the **Identities** page, click the identity whose status you want to compare.
4. In the **Edit Identity** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Displaying my identity requests

You can display requests of identities for which you are responsible. All requests that identities have made themselves or that have been made for them (for example, by a manager) are displayed.

To display requests of an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities **System entitlements**.
3. On the **Identities** page, click the identity whose requests you want to display.
4. In the **Edit Identity** pane, click the **Requests** tab.

Managing my identities' attestation cases

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

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

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

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

Detailed information about this topic

- [Displaying attestation cases of my identities](#) on page 233
- [Approving and denying attestation cases of my identities](#) on page 233

Displaying attestation cases of my identities

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

To display attestation cases

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem entitlements**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. In the **Edit Identity** pane, click the **Attestation** tab.
This displays all the identity's attestation cases.
5. (Optional) To display more details of an attestation case, click the respective attestation case.

Related topics

- [Attestation](#) on page 113
- [Displaying pending attestation cases](#) on page 137

Approving and denying attestation cases of my identities

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

To approve an attestation case

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. On the **Identities** page, click the identity whose attestation cases are pending your approval.
3. In the **Edit Identity** pane, click the **Attestation** tab.
4. On the **Attestation** tab, click ▼ (**Filter**).
5. In the filter context menu, select the **Pending** option.
6. Perform one of the following actions:
 - To approve an attestation case, select the check box next to the attestation case in the list and click **Approve** below the list.

- To deny an attestation case, select the check box next to the attestation case in the list and click **Deny** below the list.
7. In the **Approve Attestation Case** or the **Deny Attestation Case** pane, perform the following actions:
 - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
 - b. In the **Additional comments about your decision** field, enter extra information about your approval decision.
- TIP:** By giving reasons, your approvals are more transparent and support the audit trail.
8. Click **Save**.

Related topics

- [Attestation](#) on page 113
- [Approving or denying attestation cases](#) on page 138

Displaying my identities' rule violations

You can display the rule violations of identities for which you are responsible.

You can also display mitigating controls for each rule violation.

To display identities' rule violations

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities**.
3. On the **Identities** page, click the identity whose rule violations you want to display.
4. In the **Edit Identity** pane, click the **Rule Violations** tab.
5. (Optional) To display the mitigating controls of a rule violation, click **View mitigating controls** next to the rule violation.

Related topics

- [Displaying compliance rules](#) on page 152

Managing my cost centers

You can perform a variety of actions on cost centers that you manage and gather information about them.

Detailed information about this topic

- [Displaying my cost centers](#) on page 235
- [Creating your own cost centers](#) on page 235
- [Displaying and editing my cost center main data](#) on page 236
- [Copying/splitting my cost centers](#) on page 238
- [Comparing and merging my cost centers](#) on page 239
- [Restoring my cost centers to their previous state](#) on page 240
- [Managing my cost center memberships](#) on page 241
- [Managing my cost centers' entitlements](#) on page 244
- [Displaying my cost center rule violations](#) on page 246
- [My cost center history](#) on page 246
- [Restoring my deleted cost centers](#) on page 248

Displaying my cost centers

You can display all the cost centers for which you are responsible.

To display cost centers

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
This opens the **Cost Centers** page and displays all the cost centers for which you are responsible.
3. (Optional) To display details of a cost center, click the cost center.

Creating your own cost centers

You can create new cost centers for which you are responsible.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a cost center

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click **+ Create cost center**.
4. In the **Create Cost Center** pane, enter the main data of the cost center in the respective fields.

You can edit the following main data.

Table 47: Cost center main data

Property	Description
Cost center	Enter a full, descriptive name for the cost center.
Short name	Enter a short name for the cost center.
Parent cost center	Click Select/Change and select a cost center to be the parent cost center for organizing the cost center hierarchically. If you want the cost center at the root of a cost center hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the cost center.
Deputy manager	Select an identity to act as a deputy to the cost center's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Attestors	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the cost center.
Department	Click Select/Change and select the department the cost center is primarily assigned to.
Location	Click Select/Change and select the location the cost center is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the cost center.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the cost center.
Description	Enter a description for the cost center.

5. Click **Create**.

Displaying and editing my cost center main data

You can display and edit the main data of the cost centers for which you are responsible.

To display and edit a cost center's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Cost centers**.
3. On the **Cost Centers** page, click the cost centers whose main data you want to display/edit.
4. In the **Edit Cost Center** pane.

You can edit the following main data.

Table 48: Cost center main data

Property	Description
Cost center	Enter a full, descriptive name for the cost center.
Short name	Enter a short name for the cost center.
Parent cost center	Click Select/Change and select a cost center to be the parent cost center for organizing the cost center hierarchically. If you want the cost center at the root of a cost center hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the cost center.
Deputy manager	Select an identity to act as a deputy to the cost center's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Attestors	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the cost center.
Department	Click Select/Change and select the department the cost center is primarily assigned to.
Location	Click Select/Change and select the location the cost center is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the cost center.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the cost center.
Description	Enter a description for the cost center.

5. Click **Save**.

Copying/splitting my cost centers

You can copy or move memberships and entitlements from cost centers you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a cost center or move memberships and entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities > Cost centers**.
3. On the **Cost Centers** page, click the cost center you want to copy or whose memberships and entitlements you want to move.
4. In the **Edit Cost Center** pane, click **⋮ (Actions) > Split**.
5. In the **Split** pane, in the **Type of new object** menu, select which type to give the new object.
6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

TIP: After the object has been created, you can add the remaining main data (see [Displaying and editing my department main data](#) on page 171, [Displaying and editing my business roles' main data](#) on page 202, [Displaying and editing my cost center main data](#) on page 236, or [Displaying and editing my locations' main data](#) on page 265).
7. Click **Next**.
8. In the **Select assignments to be copied or moved to the new object** step, perform the following actions:
 - To neither copy nor move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and do not copy or move to new object**. The entitlement/membership is later only available in the source object.
 - To copy or move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new object**. The entitlement/membership is included later in the source object as well as the target object.
 - To move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new object**. The entitlement/membership is later removed from the source object and only included in the target object.
9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.

Related topics

- [Managing my cost center memberships](#) on page 241
- [Managing my cost centers' entitlements](#) on page 244

Comparing and merging my cost centers

You can compare properties of cost centers that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a cost center

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Cost centers**.
3. On the **Cost Centers** page, click the cost center you want to compare and merge.
4. In the **Edit Cost Center** pane, click **⋮ (Actions) > Compare and merge**.
5. In the **Compare and Merge** pane, in the **Comparison object** field, click **Select**.
6. In the **Edit Property** pane, in the **Object type** menu, select whether you want to compare and merge the cost center with a business role, department, cost center, or location.
7. Click the relevant business role, department, cost center, or location.
8. Click **Next**.

The assigned memberships and entitlements of both objects are listed with the following information in the **View comparison result** step.

Table 49: Overview of the assignments

Column	Description
Assigned object	Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.

Column	Description
This object	<p>Shows you the assignment type of the entitlement/membership in the source or comparison object. The following assignment types are available.</p> <ul style="list-style-type: none"> • Direct • Inherited • Requested • Dynamic • Not assigned <p>For more detailed information about assigning company resources, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p>
Comparison object	

9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Merge**.

Related topics

- [Managing my cost center memberships](#) on page 241
- [Managing my cost centers' entitlements](#) on page 244

Restoring my cost centers to their previous state

You can compare the current status of a cost center that you are responsible for to its status at another time and completely or partially restore the historical state.

To restore a cost center to a previous state

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Cost centers**.
3. On the **Cost Centers** page, click the cost center you want to roll back.
4. In the **Edit Cost Center** pane, click **⌵ (Actions) > Reset to previous state**.
5. In the **Reset to Previous State** pane, in the **Comparison date** field, specify a date.
6. Click **Next**.

The **View comparison result** step shows all changes that have taken place since the given date.

7. Select the check box next to the property that you want to restore to its previous state.
8. Click **Next**.
9. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
10. Click **Next**.

Related topics

- [Managing my cost center memberships](#) on page 241
- [Managing my cost centers' entitlements](#) on page 244

Managing my cost center memberships

As soon as an identity is assigned to a cost center, the identity becomes a member in the cost center.

Detailed information about this topic

- [Displaying memberships in my cost centers](#) on page 241
- [Analyzing assignments to my cost centers](#) on page 242
- [Adding identities to my cost centers](#) on page 242
- [Removing identities from my cost centers](#) on page 244

Displaying memberships in my cost centers

You can display identities that are assigned cost centers for which you are responsible.

To display identities that are assigned a cost center

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Cost centers**.
3. On the **Cost Centers** page, click the cost center whose memberships you want to display.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To display all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my cost centers

You can display how a cost center assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center whose memberships you want to display.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click the membership to display its assignment analysis.

Adding identities to my cost centers

You can assign identities to cost centers for which you are responsible.

The following assignment options are available:

- Assignment by [request](#)
- Automatic assignment through a [dynamic role](#)
- Revoking [exclusion](#) of a member

To assign an identity to a cost center using a request

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center to which you want to add an identity.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click **Request memberships**.
7. In the **Request Memberships** pane, next to the identity to which you want to assign the cost center, select the check box.
8. Click **Request memberships**.
9. Close the **Edit Cost Center** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

Once the request has been granted approval, the identity is assigned to the cost center.

To add members automatically through a dynamic role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
 2. In the navigation, click **IdentitiesCost centers**.
 3. On the **Cost centers** page, click the cost center for which you want to create a dynamic role.
 4. In the **Edit Cost Center** pane, click the **Memberships** tab.
 5. On the **Memberships** tab, click **Automatic memberships**.
 6. Click **Create dynamic role**.
 7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:
 - a. Click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition, click **Add another condition** and repeat the steps.
 - f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.
- TIP:** To remove a condition, click  (**Delete**).
- For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.
8. Click **Save**.
 9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.
 10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.
 11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center to which you want to re-add a member.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to add again as a member.
7. Click **Remove exclusion**.

Related topics

- [Requesting products](#) on page 71

Removing identities from my cost centers

You can remove cost centers from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a cost center from an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities Cost centers**.
3. On the **Cost Centers** page, click the cost center that has a membership you want to delete.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.
6. Next to the membership you want to delete, select the check box.
7. Click **Remove**.
8. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
9. Click **Remove memberships**.

TIP: If you only selected direct memberships, confirm the prompt in the **Remove Membership** dialog with **Yes**.

Managing my cost centers' entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to cost centers you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the cost centers.

Detailed information about this topic

- [Displaying my cost center entitlements](#) on page 245
- [Adding entitlements to my cost centers](#) on page 245
- [Deleting my cost center entitlements](#) on page 246

Displaying my cost center entitlements

You can display entitlements that are assigned cost centers for which you are responsible.

To display entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center whose entitlements you want to display.
4. In the **Edit Cost Center** pane, click the **Permissions** tab.

Adding entitlements to my cost centers

You can add entitlements to cost centers for which you are responsible. You do this through requests.

To add an entitlement to a cost center

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center to which you want to add an entitlement.
4. In the **Edit Cost Center** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.
9. Close the **Edit Cost Center** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

After the request has been granted approval, the entitlement is added to the cost center.

Related topics

- [Requesting products](#) on page 71

Deleting my cost center entitlements

You can delete entitlements that are assigned cost centers for which you are responsible.

To delete an entitlement of a cost center

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center whose entitlements you want to delete.
4. In the **Edit Cost Center** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying my cost center rule violations

You can display the rule violations of cost centers for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center whose rule violations you want to display.
4. On the **Edit Cost Center** pane, click the **Rule Violations** tab.

My cost center history

The Web Portal allows you to display historical data of cost centers for which you are responsible.

To do this, you have the following options:

Table 50: Historical data

View	Description
Events	Shows all events relating to the cost center in table form (see Displaying my cost center history on page 247).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my cost centers on page 247).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my cost centers on page 248).

Displaying my cost center history

To track changes, you can display the history of cost centers for which you are responsible.

To display the history

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center whose history you want to display.
4. In the **Edit Cost Center** pane, click the **History** tab.

Displaying the status overview of my cost centers

You can display all the changes effecting cost centers for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center whose status overview you want to display.
4. In the **Edit Cost Center** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of my cost centers

You can compare the current status of a cost center that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost Centers** page, click the cost center whose status you want to compare.
4. In the **Edit Cost Center** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Restoring my deleted cost centers

You can restore deleted cost centers for which you were responsible. For example, a cost center can be deleted if two roles are merged (see [Comparing and merging my cost centers](#) on page 239).

To restore a deleted cost center

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesCost centers**.
3. On the **Cost centers** page, click **Restore deleted object**.
4. In the **Restore Deleted Object** pane, click the cost center that you want to restore.
5. Click **Next**.
6. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
7. Click **Next**.

Managing my multi-request resources

The One Identity Manager distinguishes between single or multiple requestable products. Single request products are, for example, software, system roles, or Active Directory groups. These products cannot be requested if they have already been requested for the same time period.

Furthermore, an identity may need several of one type of company resources, for example, consumables like pens or printer paper. You can find company resources such as these

mapped in One Identity Manager as Multi-request resource or Multi requestable/unsubscribable resources.

Multi-request resources are automatically unsubscribed after the request is granted approval. The resources are not explicitly assigned to identities.

You can perform a variety of actions on the multi-request resources that you manage and gather information about them.

Detailed information about this topic

- [Displaying my multi-request resources](#) on page 249
- [Displaying and editing my multi-request resources' main data](#) on page 249

Displaying my multi-request resources

You can display all the multi-request resources for which you are responsible.

To display multi-request resources

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Multi-request resources**.
This opens the **Multi-request Resources** page and displays all the multi-request resources for which you are responsible.
3. (Optional) To display details of a multi-request resource, click the multi-request resource.

Displaying and editing my multi-request resources' main data

You can display and edit the main data of the multi-request resources for which you are responsible.

To display and edit a multi-request resource's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose main data you want to display/edit.
4. In the **Edit Multi-Request Resource** pane.

You can edit the following main data.

Table 51: Multi-request resource main data

Property	Description
Multi-request resource	Enter a full, descriptive name for the multi-request resource.
Resource type	Select the resource type of the multi-request resource. Use resource types to group multi-request resources.
Description	Enter a description for the multi-request resource.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning multi-request resources to identities. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Product owner	Click Select/Change and then select an application role. The members of this application role can edit the main data of the multi-request resource and be used as approvers in approval processes for multi-request resource requests.

5. Click **Save**.

Managing my multi requestable/unsubscribable resources

The One Identity Manager distinguishes between single or multiple requestable products. Single request products are, for example, software, system roles, or Active Directory groups. These products cannot be requested if they have already been requested for the same time period.

Furthermore, an identity may need several of one type of company resources, for example, consumables like pens or printer paper. You can find company resources such as these mapped in One Identity Manager as Multi-request resource or Multi requestable/unsubscribable resources.

The resources are assigned to identities after approval has been granted and they remain assigned until the request is unsubscribed. An example of multi requestable/unsubscribable resources would be printers or monitors.

You can perform a variety of actions on the multi requestable/unsubscribable resources that you manage and gather information about them.

Detailed information about this topic

- [Displaying my multi requestable/unsubscribable resources](#) on page 251
- [Displaying and editing my multi requestable/unsubscribable resources' main data](#) on page 251

Displaying my multi requestable/unsubscribable resources

You can display all the multi requestable/unsubscribable resources for which you are responsible.

To display multi requestable/unsubscribable resources

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesMulti requestable/unsubscribable resources**.
This opens the **Multi requestable/unsubscribable Resources** page and displays all the multi requestable/unsubscribable resources for which you are responsible.
3. (Optional) To display details of a multi requestable/unsubscribable resource, click the multi requestable/unsubscribable resource.

Displaying and editing my multi requestable/unsubscribable resources' main data

You can display and edit the main data of the multi requestable/unsubscribable resources for which you are responsible.

To display and edit a multi requestable/unsubscribable resource's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesMulti requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose main data you want to display/edit.
4. In the **Edit Multi Requestable/Unsubscribable Resource** pane.

You can edit the following main data.

Table 52: Multi requestable/unsubscribable resource main data

Property	Description
Multi requestable/unsubscribable resource	Enter a full, descriptive name for the multi requestable/unsubscribable resource.
Resource type	Select the resource type of the multi requestable/unsubscribable resource. Use resource types to group multi requestable/unsubscribable resources.
Description	Enter a description for the multi requestable/unsubscribable resource.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning multi requestable/unsubscribable resources to identities. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Product owner	Click Select/Change and then select an application role. The members of this application role can edit the main data of the multi requestable/unsubscribable resource and be used as approvers in approval processes for multi requestable/unsubscribable resource requests.

5. Click **Save**.

Managing my resources

An identity can own resources just 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 a later point. For example, a resource could be a telephone or a company car.

You can perform a variety of actions on resources that you manage and gather information about them.

Detailed information about this topic

- [Displaying my resources](#) on page 253
- [Displaying and editing my resources' main data](#) on page 253

Displaying my resources

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

To display resources

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesResources**.
This opens the **Resources** page and displays all the resources for which you are responsible.
3. (Optional) To display details of a resource, click the resource.

Displaying and editing my resources' main data

You can display and edit the main data of the resources for which you are responsible.

To display and edit a resource's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesResources**.
3. On the **Resources** page, click the resource whose main data you want to display/edit.
4. In the **Edit Resource** pane.

You can edit the following main data.

Table 53: Resource main data

Property	Description
Resource	Enter a full, descriptive name for the resource.
Resource type	Select a resource type for the resource. Use resource types to group resources.
Description	Enter a description for the resource.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning resources to identities. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Product owner	Click Select/Change and then select an application role. The members of this application role can edit the main data of the resource and be used as approvers in approval processes for resource requests.

5. Click **Save**.

Managing my software applications

Software applications can be assigned directly or indirectly to identities. Indirect assignment is carried out by allocating identities and software applications in company structures, like departments, cost centers, locations, or business roles. Examples of software application that can be assigned are: internet, address management, email or text editing software.

You can perform a variety of actions on the software applications that you manage and gather information about them.

Detailed information about this topic

- [Displaying my software applications](#) on page 254
- [Displaying and editing my software applications' main data](#) on page 255
- [Managing my software application memberships](#) on page 257

Displaying my software applications

You can display all the software applications for which you are responsible.

To display software applications

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Software**.
This opens the **Software** page and displays all the software applications for which you are responsible.
3. (Optional) To display details of a software application, click the software application.

Displaying and editing my software applications' main data

You can display and edit the main data of the software applications for which you are responsible.

To display and edit a software application's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Software**.
3. On the **Software** page, click the software application whose main data you want to display/edit.
4. In the **Edit Software Application** pane.

You can edit the following main data.

Table 54: Software application main data

Property	Description
Software name	Enter a full, descriptive name for the software application.
Version	Enter the version of the software application.
Language	Click Select/Change and select the software application's language.
Service item	<p>Click Create a new service item and create a new service item (a product).</p> <p>If a service item is already assigned, click Change and select a service item.</p> <p>You cannot use a software application until a service item has been assigned to it.</p>
Internal product name	Enter a company internal name for the software application.
Website.	Enter the URL of the manufacturer's product website.
Link to documentation	Enter the URL of the documentation website.
Description	Enter a description for the software application.
Comment	Enter a comment for the software application.
IT shop	Select the check box if the software application can be requested through the IT Shop. This software application can be requested by identities using the Web Portal and allocated by defined approval processes. The software application can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only use in IT Shop	Select the check box if the software application can only be requested through the IT Shop. This software application can be requested by identities using the Web Portal and allocated by defined approval processes. The software may not be assigned directly to hierarchical roles.
Disabled	Select the check box if the software application is not used. Only enabled software applications can be assigned in One Identity Manager. If a software application is disabled, the software cannot be assigned but any existing assignments are upheld.

5. Click **Save**.

Displaying my software application owners

You can specify which identities are responsible for your software applications. To do this, you must assign one or more product owners to the service item assigned to the software application.

To specify owners for a software application

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSoftware**.
3. On the **Software** page, click the software application for which you want specify an owner.
4. In the **Edit Software** pane, click the **Service Item** tab.
5. On the **Service Item** tab, perform one of the following actions:
 - To specify members of a specific application role as product owners, perform the following actions:
 1. Under **Product owner**, enable the **Select from roles** option.
 2. In the **Product owner** field, click **Select/Change**.
 3. In the **Edit Property** pane, click the appropriate application role.
 - To specify a specific identity as the product owner, perform the following actions:
 1. Under **Product owner**, enable the **Select from identities** option.
 2. In the **Identity** list, select the corresponding identity.
6. Click **Save**.

Managing my software application memberships

As soon as a software application is assigned to an identity, the identity becomes a member in the software application.

Detailed information about this topic

- [Displaying memberships in my software applications](#) on page 258
- [Analyzing assignments to my software applications](#) on page 258
- [Assigning identities to my software applications](#) on page 258
- [Removing identities from my software applications](#) on page 259

Displaying memberships in my software applications

You can display identities that are assigned software application for which you are responsible.

To display identities that are assigned a software application

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSoftware**.
3. On the **Software** page, click the software application whose memberships you want to display.
4. In the **Edit Software** pane, click the **Memberships** tab.

Analyzing assignments to my software applications

You can display how a software application assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSoftware**.
3. On the **Software** page, click the software application whose memberships you want to display.
4. In the **Edit Software** pane, click the **Memberships** tab.
5. Click the membership to display its assignment analysis.

Assigning identities to my software applications

You can assign identities to software applications for which you are responsible. You do this with a request.

To assign an identity to a software application using a request

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSoftware**.
3. On the **Software** page, click the software application to which you want to assign an identity.
4. In the **Edit Software Application** pane, click the **Memberships** tab.
5. In the **Request Memberships** pane, next to the identity to which you want to assign the software application, select the check box.
6. Click **Request memberships**.
7. Close the **Edit Software Application** pane.

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

Once the request has been granted approval, the identity is assigned to the software application.

Related topics

- [Requesting products](#) on page 71

Removing identities from my software applications

You can remove software applications from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a software application from an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSoftware**.
3. On the **Software** page, click the software application that has a membership you want to delete.
4. In the **Edit Software** pane, click the **Memberships** tab.
5. Next to the membership you want to delete, select the check box.
6. Perform one of the following actions:
 - If it is a direct assignment, click **Delete**.
 - If it is an assignment request, click **Unsubscribe**.

NOTE: You can only unsubscribe memberships that you have requested yourself.

7. In the **Remove Memberships** or **Unsubscribe Memberships** dialog, confirm the prompt with **OK**.

Managing service items of my software applications

To be able to request software applications as products, they must be allocated to service items that are assigned to a shop (see [Managing requestable products in shops](#) on page 54).

Detailed information about this topic

- [Editing service items of my software applications](#) on page 260

Editing service items of my software applications

You can edit the main data of service items.

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

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSoftware**.
3. On the **Software** page, click the software application whose service items you want to edit.
4. In the **Edit Software** pane, click the **Service Item** tab.
5. On the **Service Item** tab, edit the service item's main data.

You can edit the following main data.

Table 55: Service item main data

Property	Description
Service item	Enter a name for the service item.
Description	Enter a description of the service item.
Service category	You can group different service items into service categories. To do this, click /Select/Change and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 56.
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Approval by multi-factor authentication	Select this check box if approvals of requests for this service item require multi-factor authentication.
Max. days valid	Specify how long an identity can keep the product until it is automatically unsubscribed again. An identity keeps their requested products on the shelf until they unsubscribe from them themselves. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. Products that are intended to have a limited shelf life need to be marked with a validity period.
Website	Specify the URL of a web page that contains more information about the product. Use the following format: https://www.example.com or http://www.example.com .

Property	Description
	This field allows you to link product descriptions in the internet or intranet to the service item.
Sort order	Specify how the service category is sorted.
Request property	<p>Select the request property using the additional request parameters that are defined for a request. If you do not select any request properties, the request properties of the associated service category are used.</p> <p>Requests can be given additional information though product-specific request properties such as the specific details of a product, its size, or color. A request property gathers all additional features together that can be given when requesting a product.</p>
Functional area	<p>Click Select/Change and then select the functional area to which you want to assign the service item.</p> <p>You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by functional area. To do this, service items must be assigned to functional areas. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p>
Attestor	Click Select/Change and then select an application role. Members of this application role can approve attestation cases that affect the service item.
Terms of use	Select the terms of use that the product's requester must accept.
Reason type on request	<p>Select which type of reason is required when the service item is requested.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on approval	<p>Select which type of reason is required when the service item request is approved.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with

Property	Description
	<p>any text.</p> <ul style="list-style-type: none"> Free text required: A reason must be given with freely selected text.
Reason type on denial	<p>Select which type of reason is required when the service item request is denied.</p> <ul style="list-style-type: none"> Optional: A reason can be provided if required. Reason required (standard or free): A standard reason must be selected or a reason given with any text. Free text required: A reason must be given with freely selected text.
Picture	<p>Enter a picture for the service item. Users see this picture when they make a request.</p> <p>Perform the following actions as well:</p> <ol style="list-style-type: none"> Click Add/Change. Select an image from your medium.
Hide in service catalog	<p>Set this check box if the service item is meant to be requestable but is not displayed in the service catalog.</p>
Request parameters must be defined per recipient	<p>Select the check box to enter additional request properties separately for each recipient of the associated product, if the product is requested for several recipients in one request procedure.</p>
Retain service item assignment on relocation	<p>Select the check box if you want requests for this service item to be retained when a customer or the product is moved.</p> <p>If an identity requests a product from a shop and changes the shop at a later date, a decision must be made about how to proceed with the existing request. The same applies if a product is moved to another shelf.</p>
Tags	<p>Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.</p>
Not requestable/Requestable	<p>Set the switch to Requestable if you want to request the product via the Web Portal.</p> <p>Set the switch to Not requestable if you do not want to request the product via the Web Portal.</p>

Property	Description
Product owner	<p>Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item.</p> <p>Specify which identities are responsible for the service item.</p> <ul style="list-style-type: none"> • To specify members of a specific application role as product owners, perform the following actions: <ol style="list-style-type: none"> 1. Under Product owner, enable the Select from roles option. 2. In the Product owner field, click Select/Change. 3. In the Edit Property pane, click the appropriate application role. • To specify a specific identity as the product owner, perform the following actions: <ol style="list-style-type: none"> 1. Under Product owner, enable the Select from identities option. 2. In the Identity list, select the corresponding identity.

6. Click **Save**.

Related topics

- [Displaying my software application owners](#) on page 257

Managing my locations

You can perform a variety of actions on locations that you manage and gather information about them.

Detailed information about this topic

- [Displaying my locations](#) on page 264
- [Creating your own locations](#) on page 264
- [Displaying and editing my locations' main data](#) on page 265
- [Copying/splitting my locations](#) on page 267
- [Comparing and merging my locations](#) on page 268

- [Restoring my locations to their previous state](#) on page 269
- [Managing my location memberships](#) on page 270
- [Managing my locations' entitlements](#) on page 273
- [Displaying my locations' rule violations](#) on page 275
- [My locations' history](#) on page 275
- [Restoring my deleted locations](#) on page 277

Displaying my locations

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

To display locations

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Locations**.
This opens the **Locations** page and displays all the locations for which you are responsible.
3. (Optional) To display details of a location, click the location.

Creating your own locations

You can create new locations for which you are responsible.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a location

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Locations**.
3. On the **Locations** page, click **+ Create locations**.
4. In the **Create Location** pane, enter the main data of the location in the respective fields.

You can edit the following main data.

Table 56: Location main data

Property	Description
Location	Enter a full, descriptive name for the location.
Short name	Enter a short name for the location.
Name	Enter an additional description for the location.
Parent location	Click Select/Change and select a location to be the parent location for organizing the location hierarchically. If you want the location at the root of a location hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the location.
Deputy manager	Select an identity to act as a deputy to the location's manager.
Additional manager	Click Select/Change and select an application role. Members of the selected application role are responsible for the location.
Attestor	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the location.
Department	Click Select/Change and select the department the location is primarily assigned to.
Cost center	Click Select/Change and select the cost center the location is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the location.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the location.
Description	Enter a description for the location.

5. Click **Create**.

Displaying and editing my locations' main data

You can display and edit the main data of the locations for which you are responsible.

To display and edit a location's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the locations whose main data you want to display/edit.
4. In the **Edit Location** pane.

You can edit the following main data.

Table 57: Location main data

Property	Description
Location	Enter a full, descriptive name for the location.
Short name	Enter a short name for the location.
Name	Enter an additional description for the location.
Parent location	Click Select/Change and select a location to be the parent location for organizing the location hierarchically. If you want the location at the root of a location hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the location.
Deputy manager	Select an identity to act as a deputy to the location's manager.
Additional manager	Click Select/Change and select an application role. Members of the selected application role are responsible for the location.
Attestor	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the location.
Department	Click Select/Change and select the department the location is primarily assigned to.
Cost center	Click Select/Change and select the cost center the location is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the location.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the location.
Description	Enter a description for the location.

5. Click **Save**.

Copying/splitting my locations

You can copy or move memberships and entitlements from locations you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a location or move memberships and entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location you want to copy or whose memberships and entitlements you want to move.
4. In the **Edit Location** pane, click **⋮ (Actions) > Split**.
5. In the **Split** pane, in the **Type of new object** menu, select which type to give the new object.
6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

TIP: After the object has been created, you can add the remaining main data (see [Displaying and editing my department main data](#) on page 171, [Displaying and editing my business roles' main data](#) on page 202, [Displaying and editing my cost center main data](#) on page 236, or [Displaying and editing my locations' main data](#) on page 265).
7. Click **Next**.
8. In the **Select assignments to be copied or moved to the new object** step, perform the following actions:
 - To neither copy nor move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and do not copy or move to new object**. The entitlement/membership is later only available in the source object.
 - To copy or move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new object**. The entitlement/membership is included later in the source object as well as the target object.
 - To move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new object**. The entitlement/membership is later removed from the source object and only included in the target object.
9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.

Related topics

- [Managing my location memberships](#) on page 270
- [Managing my locations' entitlements](#) on page 273

Comparing and merging my locations

You can compare properties of locations that you are responsible for, with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a location

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location you want to compare and merge.
4. In the **Edit Location** pane, click **⋮ (Actions) > Compare and merge**.
5. In the **Compare and Merge** pane, in the **Comparison object** field, click **Select**.
6. In the **Edit Property** pane, in the **Object type** menu, select whether you want to compare and merge the location with a business role, department, cost center, or location.
7. Click the relevant business role, department, cost center, or location.
8. Click **Next**.

The assigned memberships and entitlements of both objects are listed with the following information in the **View comparison result** step.

Table 58: Overview of the assignments

Column	Description
Assigned object	Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.

Column	Description
This object	<p>Shows you the assignment type of the entitlement/membership in the source or comparison object. The following assignment types are available.</p> <ul style="list-style-type: none"> • Direct • Inherited • Requested • Dynamic • Not assigned <p>For more detailed information about assigning company resources, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p>
Comparison object	

9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Merge**.

Related topics

- [Managing my location memberships](#) on page 270
- [Managing my locations' entitlements](#) on page 273

Restoring my locations to their previous state

You can compare the current status of a location that you are responsible for to its status at another time and completely or partially restore the historical state.

To restore a location to a previous state

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location you want to roll back.
4. In the **Edit Location** pane, click **(Actions) > Reset to previous state**.
5. In the **Reset to Previous State** pane, in the **Comparison date** field, specify a date.
6. Click **Next**.

The **View comparison result** step shows all changes that have taken place since the given date.

7. Select the check box next to the property that you want to restore to its previous state.
8. Click **Next**.
9. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
10. Click **Next**.

Related topics

- [Managing my location memberships](#) on page 270
- [Managing my locations' entitlements](#) on page 273

Managing my location memberships

As soon as an identity is assigned to a location, the identity becomes a member in the location.

Detailed information about this topic

- [Displaying memberships in my locations](#) on page 270
- [Analyzing assignments to my locations](#) on page 271
- [Adding identities to my locations](#) on page 271
- [Removing identities from my locations](#) on page 273

Displaying memberships in my locations

You can display identities that are assigned locations for which you are responsible.

To display identities that are assigned a location

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location whose memberships you want to display.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To display all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to my locations

You can display how a location assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Locations**.
3. On the **Locations** page, click the location whose memberships you want to display.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click the membership to display its assignment analysis.

Adding identities to my locations

You can assign identities to locations for which you are responsible.

The following assignment options are available:

- Assignment by [request](#)
- Automatic assignment through a [dynamic role](#)
- Revoking [exclusion](#) of a member

To assign an identity to a location using a request

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Locations**.
3. On the **Locations** page, click the location to which you want to add an identity.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click **Request memberships**.
7. In the **Request Memberships** pane, next to the identity to which you want to assign the location, select the check box.
8. Click **Request memberships**.
9. Close the **Edit Location** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

Once the request has been granted approval, the identity is assigned to the location.

To add members automatically through a dynamic role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
 2. In the navigation, click **IdentitiesLocations**.
 3. On the **Locations** page, click the location for which you want to create a dynamic role.
 4. In the **Edit Location** pane, click the **Memberships** tab.
 5. On the **Memberships** tab, click **Automatic memberships**.
 6. Click **Create dynamic role**.
 7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:
 - a. Click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition, click **Add another condition** and repeat the steps.
 - f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.
- TIP:** To remove a condition, click  (**Delete**).
- For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.
8. Click **Save**.
 9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.
 10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.
 11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location to which you want to re-add a member.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.
6. Select the check box next to the identity you want to add again as a member.
7. Click **Remove exclusion**.

Related topics

- [Requesting products](#) on page 71

Removing identities from my locations

You can remove locations from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a location from an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities****Locations**.
3. On the **Locations** page, click the location that has a membership you want to delete.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. Next to the membership you want to delete, select the check box.
6. Click **Remove**.
7. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
8. Click **Remove memberships**.

TIP: If you only selected direct memberships, confirm the prompt in the **Remove Membership** dialog with **Yes**.

Managing my locations' entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to locations you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the locations.

Detailed information about this topic

- [Displaying my locations' entitlements](#) on page 274
- [Adding entitlements to my locations](#) on page 274
- [Deleting my locations' entitlements](#) on page 274

Displaying my locations' entitlements

You can display entitlements that are assigned locations for which you are responsible.

To display entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location whose entitlements you want to display.
4. In the **Edit Locations** pane, click the **Permissions** tab.

Adding entitlements to my locations

You can add entitlements to locations for which you are responsible. You do this through requests.

To add an entitlement to a location

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location to which you want to add an entitlement.
4. In the **Edit Locations** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.
9. Close the **Edit Location** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

After the request has been granted approval, the entitlement is added to the location.

Related topics

- [Requesting products](#) on page 71

Deleting my locations' entitlements

You can delete entitlements that are assigned locations for which you are responsible.

To delete an entitlement of a location

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location whose entitlements you want to delete.
4. In the **Edit Locations** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying my locations' rule violations

You can display the rule violations of locations for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location whose rule violations you want to display.
4. On the **Edit Location** pane, click the **Rule Violations** tab.

My locations' history

The Web Portal allows you to display historical data of locations for which you are responsible.

To do this, you have the following options:

Table 59: Historical data

View	Description
Events	Shows all events relating to the location in table form (see Displaying my locations' history on page 276).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my locations on page 276).
Status comparison	You can select a date and display all the changes made from then

View	Description
	until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my locations on page 276).

Displaying my locations' history

To track changes, you can display the history of locations for which you are responsible.

To display the history

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location whose history you want to display.
4. In the **Edit Location** pane, click the **History** tab.

Displaying the status overview of my locations

You can display all the changes effecting locations for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location whose status overview you want to display.
4. In the **Edit Location** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of my locations

You can compare the current status of a location that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click the location whose status you want to compare.
4. In the **Edit Location** pane, click the **History** tab.

5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Restoring my deleted locations

You can recover deleted locations for which you were responsible. For example, a location can be deleted if two roles are merged (see [Comparing and merging my locations](#) on page 268).

To restore a deleted location

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesLocations**.
3. On the **Locations** page, click **Restore deleted object**.
4. In the **Restore Deleted Object** pane, click the location that you want to restore.
5. Click **Next**.
6. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
7. Click **Next**.

Managing my 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.

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

You could manage the following system entitlements:

- Active Directory groups
- SAP groups
- SharePoint groups
- PAM groups

Detailed information about this topic

- [Displaying my system entitlements](#) on page 278
- [Displaying and editing my system entitlements' main data](#) on page 278
- [Creating reports about my system entitlements](#) on page 279

- [Making my system entitlements requestable](#) on page 280
- [Managing my system entitlements' service items](#) on page 281
- [Managing my system entitlement memberships](#) on page 285
- [Managing my system entitlements' child groups](#) on page 287
- [My system entitlements' history](#) on page 288
- [Managing my system entitlements' attestation cases](#) on page 290

Displaying my system entitlements

You can display all the system entitlements for which you are responsible.

To display system entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
This opens the **System Entitlements** page and displays all the system entitlements for which you are responsible.
3. (Optional) To display only system entitlements that are assigned to a specific target system, perform the following actions:
 - a. Click  (**target system**).
 - b. In the **Narrow the selection further down by: Target system** dialog, select the target system whose system entitlements you want to display.
TIP: To display target systems that are under a target system, click  (**expand**).
4. (Optional) To display details of a system entitlement, click the system entitlement.

Displaying and editing my system entitlements' main data

You can display and edit the main data of the system entitlements for which you are responsible.

To display and edit a system entitlement's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlements whose main data you want to display/edit.
4. In the **Edit System Entitlement** pane.

You can edit the following main data.

Table 60: System entitlement main data

Property	Description
Name	Enter a full, descriptive name for the system entitlement.
Canonical name	Shows the automatically generated canonical name of the system entitlement.
Distinguished name	Shows the automatically generated distinguished name of the system entitlement.
Display name	Enter a name for displaying the system entitlement in the One Identity Manager tools.
Notes domain	Shows the Notes domain name.
Description	Enter a description for the system entitlement.
Category	Select the category for system entitlement inheritance. User accounts can inherit system entitlements selectively. To do this, system entitlements and user accounts are divided into categories.
IT shop	Enable this check box to allow the system entitlement to be requested through the IT Shop. This system entitlement can be requested by your identities through the Web Portal and allocated by defined approval processes. The system entitlement can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only use in IT Shop	Enable the check box to allow the system entitlement to be requested through the IT Shop if required. This system entitlement can be requested by your identities through the Web Portal and allocated by defined approval processes. The system entitlement may not be assigned directly to hierarchical roles.

5. Click **Save**.

Creating reports about my system entitlements

You can create reports about system entitlement data.

To create a report about a system entitlement

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.

3. On the **System Entitlements** page, click the system entitlement for which you want to create a report.
4. In the **Edit System Entitlements** pane, click the **Download report** tab.

Making my system entitlements requestable

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

- The system entitlement must be assigned to a service item (see [Managing my system entitlements' service items](#) on page 281).
- The system entitlement must be assigned to a shelf in a shop (see [Adding products to shelves](#) on page 55).
- The system entitlement must be marked as requestable (see following step-by-step).

To make a system entitlement requestable

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. (Optional) To display only those system entitlements that are not marked as requestable, perform the following actions:
 - a. Click **▼ (Filter)**.
 - b. In the filter context menu, select the **Not requestable** check box.
4. In the list, select the check box in front of the system entitlement that you want to make requestable.
5. Click **⋮ (Actions) > Make requestable**.

TIP: If you do not want the system entitlement to be requested in the Web Portal anymore, click **⋮ (Actions) > Make not requestable**.

Related topics

- [Managing shops](#) on page 46
- [Managing my system entitlements' service items](#) on page 281
- [Adding products to shelves](#) on page 55

Specifying my system entitlement owners

You can specify which identities are responsible for your system entitlements. To do this, you must assign one or more product owners to the service item assigned to the system entitlement.

To specify owners for a system entitlement

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlement whose owners you want to specify.
4. In the **Edit System EntitlementEdit Software** pane, click the tab.
5. On the **Service Item** tab, perform one of the following actions:
 - To specify members of a specific application role as product owners, perform the following actions:
 1. Under **Product owner**, enable the **Select from roles** option.
 2. In the **Product owner** field, click **Select/Change**.
 3. In the **Edit Property** pane, click the appropriate application role.
 - To specify a specific identity as the product owner, perform the following actions:
 1. Under **Product owner**, enable the **Select from identities** option.
 2. In the **Identity** list, select the corresponding identity.
6. Click **Save**.

Managing my system entitlements' service items

To be able to request system entitlements as products, they must be allocated to service items that are assigned to a shop (see [Managing requestable products in shops](#) on page 54).

Detailed information about this topic

- [Specifying my system entitlement owners](#) on page 280
- [Editing my system entitlements' service items](#) on page 281

Editing my system entitlements' service items

You can edit the main data of service items.

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

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlement whose service item you want to edit.
4. In the **Edit System EntitlementEdit Software** pane, click the tab.

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

You can edit the following main data.

Table 61: Service item main data

Property	Description
Service item	Enter a name for the service item.
Description	Enter a description of the service item.
Service category	You can group different service items into service categories. To do this, click /Select/Change and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 56.
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Approval by multi-factor authentication	Select this check box if approvals of requests for this service item require multi-factor authentication.
Max. days valid	Specify how long an identity can keep the product until it is automatically unsubscribed again. An identity keeps their requested products on the shelf until they unsubscribe from them themselves. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. Products that are intended to have a limited shelf life need to be marked with a validity period.
Website	Specify the URL of a web page that contains more information about the product. Use the following format: https://www.example.com or http://www.example.com . This field allows you to link product descriptions in the internet or intranet to the service item.
Sort order	Specify how the service category is sorted.
Request property	Select the request property using the additional request parameters that are defined for a request. If you do not select any request properties, the request properties of the associated service category are used. Requests can be given additional information though product-specific request properties such as the

Property	Description
	specific details of a product, its size, or color. A request property gathers all additional features together that can be given when requesting a product.
Functional area	<p>Click Select/Change and then select the functional area to which you want to assign the service item.</p> <p>You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by functional area. To do this, service items must be assigned to functional areas. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p>
Attestor	Click Select/Change and then select an application role. Members of this application role can approve attestation cases that affect the service item.
Terms of use	Select the terms of use that the product's requester must accept.
Reason type on request	<p>Select which type of reason is required when the service item is requested.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on approval	<p>Select which type of reason is required when the service item request is approved.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on denial	<p>Select which type of reason is required when the service item request is denied.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with

Property	Description
	<p>any text.</p> <ul style="list-style-type: none"> Free text required: A reason must be given with freely selected text.
Picture	<p>Enter a picture for the service item. Users see this picture when they make a request.</p> <p>Perform the following actions as well:</p> <ol style="list-style-type: none"> Click Add/Change. Select an image from your medium.
Hide in service catalog	<p>Set this check box if the service item is meant to be requestable but is not displayed in the service catalog.</p>
Request parameters must be defined per recipient	<p>Select the check box to enter additional request properties separately for each recipient of the associated product, if the product is requested for several recipients in one request procedure.</p>
Retain service item assignment on relocation	<p>Select the check box if you want requests for this service item to be retained when a customer or the product is moved.</p> <p>If an identity requests a product from a shop and changes the shop at a later date, a decision must be made about how to proceed with the existing request. The same applies if a product is moved to another shelf.</p>
Tags	<p>Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.</p>
Not requestable/Requestable	<p>Set the switch to Requestable if you want to request the product via the Web Portal.</p> <p>Set the switch to Not requestable if you do not want to request the product via the Web Portal.</p>
Product owner	<p>Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item.</p> <p>Specify which identities are responsible for the service item.</p> <ul style="list-style-type: none"> To specify members of a specific application role as product owners, perform the following actions: <ol style="list-style-type: none"> Under Product owner, enable the Select

Property	Description
	<p>from roles option.</p> <ol style="list-style-type: none"> In the Product owner field, click Select/Change. In the Edit Property pane, click the appropriate application role. <ul style="list-style-type: none"> To specify a specific identity as the product owner, perform the following actions: <ol style="list-style-type: none"> Under Product owner, enable the Select from identities option. In the Identity list, select the corresponding identity.

6. Click **Save**.

Related topics

- [Specifying my system entitlement owners](#) on page 280

Managing my system entitlement memberships

As soon as a system entitlement has been assigned to an identity using a corresponding user account, the identity becomes a member in the system entitlement.

Detailed information about this topic

- [Displaying memberships in my system entitlements](#) on page 285
- [Analyzing assignments to my system entitlements](#) on page 286
- [Assigning identities to my system entitlements](#) on page 286
- [Removing identities from my system entitlements](#) on page 287

Displaying memberships in my system entitlements

You can display identities that are assigned system entitlements for which you are responsible.

To display identities that are assigned a system entitlement

- In the menu bar, click **Responsibilities > My Responsibilities**.
- In the navigation, click Identities.

3. On the **System Entitlements** page, click the system entitlement whose memberships you want to display.
4. In the **Edit System Entitlement** pane, click the **Memberships** tab.
5. (Optional) To display all memberships that were created directly in the selected system entitlement, click **Direct memberships**.
6. (Optional) To display all memberships created by inheritance from child system entitlements, click **Inherited memberships**.

Analyzing assignments to my system entitlements

You can display how a system entitlement assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlement whose memberships you want to display.
4. In the **Edit System Entitlement** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Direct memberships** or **Inherited memberships**.
6. Click the membership to display its assignment analysis.

Assigning identities to my system entitlements

You can assign identities to system entitlements for which you are responsible. You do this with a request.

To assign an identity to a system entitlement using a request

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlement to which you want to assign an identity.
4. In the **Edit System Entitlement** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Request memberships**.
6. In the **Request Memberships** pane, next to the identity to which you want to assign the system entitlement, select the check box.
7. Click **Apply**.
8. Close the **Edit System Entitlement** pane.
9. In the menu bar, click **Requests > Shopping cart**.

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

Once the request has been granted approval, the identity is assigned to the system entitlement.

Related topics

- [Requesting products](#) on page 71

Removing identities from my system entitlements

You can remove system entitlements from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a system entitlement from an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities**.
3. On the **System Entitlements** page, click the system entitlement that has a membership you want to delete.
4. In the **Edit System Entitlement** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Direct Memberships**.
6. Next to the membership you want to delete, select the check box.
7. Perform one of the following actions:
 - If it is a direct assignment, click **Delete**.
 - If it is an assignment request, click **Unsubscribe**.

NOTE: You can only unsubscribe memberships that you have requested yourself.

8. In the **Remove Memberships** or **Unsubscribe Memberships** dialog, confirm the prompt with **OK**.

Managing my system entitlements' child groups

You can order more groups under certain group types or order these under other groups:

- Active Directory groups
- LDAP groups
- Notes groups
- Custom target systems groups

Detailed information about this topic

- [Display my system entitlements' child groups](#) on page 288

Display my system entitlements' child groups

You can display all groups that are child groups of the system entitlements for which You are responsible.

To display the child groups of a system entitlement

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlement whose child groups you want to display.
4. In the **Edit System Entitlement** pane, click the **Child System Entitlements** tab.

My system entitlements' history

The Web Portal allows you to display historical data of system entitlements for which you are responsible.

To do this, you have the following options:

Table 62: Historical data

View	Description
Events	Shows all events relating to the system entitlement in table form (see Displaying my system entitlements' history on page 288).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status my system entitlements' overview on page 289).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my system entitlements on page 289).

Displaying my system entitlements' history

To track changes, you can display the history of system entitlements for which you are responsible.

To display the history

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlement whose history you want to display.
4. In the **Edit System Entitlement** pane, click the **History** tab.

Displaying the status my system entitlements' overview

You can display all the changes effecting system entitlements for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlement whose status overview you want to display.
4. In the **Edit System Entitlement** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of my system entitlements

You can compare the current status of a system entitlement that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlement whose status you want to compare.
4. In the **Edit System Entitlement** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Managing my system entitlements' attestation cases

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

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

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

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

Detailed information about this topic

- [Displaying my system entitlements' attestation cases](#) on page 290
- [Approving and denying my system entitlements' attestation cases](#) on page 291

Displaying my system entitlements' attestation cases

You can display attestation cases that involve system entitlements for which you are responsible.

In addition, you can obtain more information about the attestation cases.

To display attestation cases

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. In the **Edit System Entitlement** pane, click the **Attestation** tab.
This displays all the system entitlement's attestation cases.
5. (Optional) To display more details of an attestation case, click the respective attestation case.

Related topics

- [Attestation](#) on page 113
- [Displaying pending attestation cases](#) on page 137

Approving and denying my system entitlements' attestation cases

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

To approve an attestation case

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. On the **System Entitlements** page, click the system entitlement whose attestation cases are pending your approval.
3. In the **Edit System Entitlement** pane, click the **Attestation** tab.
4. On the **Attestation** tab, click **▼ (Filter)**.
5. In the filter context menu, select the **Pending** option.
6. Perform one of the following actions:
 - To approve an attestation case, select the check box next to the attestation case in the list and click **Approve** below the list.
 - To deny an attestation case, select the check box next to the attestation case in the list and click **Deny** below the list.
7. In the **Approve Attestation Case** or the **Deny Attestation Case** pane, perform the following actions:
 - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
 - b. In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

Related topics

- [Attestation](#) on page 113
- [Approving or denying attestation cases](#) on page 138

Managing my system roles

System roles combine company resources that must always be assigned to identities together into a single package. Different types of company resources can be grouped into one system role, such as Active Directory groups, software, and resources. System roles can be assigned to user accounts, requested, or inherited through hierarchical roles. Identities and workdesks inherit company resources assigned to the system roles.

You can perform a variety of actions regarding system roles that you manage and gather information about them.

Detailed information about this topic

- [Displaying my system roles](#) on page 292
- [Creating your own system roles](#) on page 292
- [Displaying and editing my system roles' main data](#) on page 294
- [Managing my system role memberships](#) on page 295
- [Managing my system roles' entitlements](#) on page 298
- [Displaying my system roles' rule violations](#) on page 299
- [My system roles' history](#) on page 300

Displaying my system roles

You can display all the system roles for which you are responsible.

To display system roles

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem roles**.
This opens the **System Roles** page and displays all the system roles for which you are responsible.
3. (Optional) To display details of a system role, click the system role.

Creating your own system roles

You can create new system roles for which you are responsible.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a system role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities System roles**.
3. On the **System Roles** page, click **+ Create system role**.
4. In the **Create System Role** pane, enter the main data of the system role in the respective fields.

You can edit the following main data.

Table 63: System role main data

Property	Description
System role	Enter a full, descriptive name for the system role.
Display name	Enter a name for displaying the system role in the One Identity Manager tools.
Internal product name	Enter a company internal name for the system role.
System role type	Select the role type of the system role. The system role type specifies which type of company resources make up the system role.
Service item	Shows you the associated service item.
System role manager	Click Change and select the identity responsible for the system role. This identity can edit the system role's main data and be used as an attestor for system role properties. If the system role can be requested in the IT Shop, the manager will automatically be a member of the application role for product owners assigned the service item.
Comment	Enter a comment for the system role.
IT shop	Select the check box if the system role can also be requested through the IT Shop. This system role can be requested by identities through the Web Portal and allocated by defined approval processes. The system role can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only use in IT Shop	Select the check box if the system role can only be requested through the IT Shop. This system role can be requested by identities through the Web Portal and allocated by defined approval processes. The system role may not be assigned directly to hierarchical roles.

5. Click **Create**.

Displaying and editing my system roles' main data

You can display and edit the main data of the system roles for which you are responsible.

To display and edit a system role's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities System roles**.
3. On the **System Roles** page, click the system role whose main data you want to display.
4. In the **Edit System Role** pane.

You can edit the following main data.

Table 64: System role main data

Property	Description
System role	Enter a full, descriptive name for the system role.
Display name	Enter a name for displaying the system role in the One Identity Manager tools.
Internal product name	Enter a company internal name for the system role.
System role type	Select the role type of the system role. The system role type specifies which type of company resources make up the system role.
Service item	Shows you the associated service item.
System role manager	Click Change and select the identity responsible for the system role. This identity can edit the system role's main data and be used as an attestor for system role properties. If the system role can be requested in the IT Shop, the manager will automatically be a member of the application role for product owners assigned the service item.
Comment	Enter a comment for the system role.
IT shop	Select the check box if the system role can also be requested through the IT Shop. This system role can be requested by identities through the Web Portal and allocated by defined approval processes. The system role can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only use in IT Shop	Select the check box if the system role can only be requested through the IT Shop. This system role can be requested by identities through the Web Portal and allocated by defined approval processes. The system role may not be assigned directly to hierarchical roles.

5. Click **Save**.

Managing my system role memberships

As soon as a system role is assigned to an identity, the identity becomes a member in the system role.

Detailed information about this topic

- [Displaying memberships in my system roles](#) on page 296
- [Analyzing assignments to my system roles](#) on page 296
- [Assigning identities to my system roles](#) on page 296
- [Removing identities from my system roles](#) on page 297

Displaying memberships in my system roles

You can display identities that are assigned system roles for which you are responsible.

To display identities that are assigned a system role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities **System roles**.
3. On the **System Roles** page, click the system role whose memberships you want to display.
4. In the **Edit System Role** pane, click the **Memberships** tab.

Analyzing assignments to my system roles

You can display how a system role assignment under your responsibility came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities **System roles**.
3. On the **System Roles** page, click the system role whose memberships you want to display.
4. In the **Edit System Role** pane, click the **Memberships** tab.
5. Click the membership to display its assignment analysis.

Assigning identities to my system roles

You can assign identities to system roles for which you are responsible. You do this with a request.

To assign an identity to a system role using a request

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities **System roles**.

3. On the **System Roles** page, click the system role to which you want to assign an identity.
4. In the **Edit System Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Request memberships**.
6. In the **Request Memberships** pane, next to the identity to which you want to assign the system role, select the check box.
7. Click **Request memberships**.
8. Close the **Edit System Role** pane.
9. In the menu bar, click **Requests > Shopping cart**.
10. On the **Shopping Cart** page, click **Submit**.
Once the request has been granted approval, the identity is assigned to the system role.

Related topics

- [Requesting products](#) on page 71

Removing identities from my system roles

You can remove system roles from identities, for which you are responsible, by deleting or unsubscribing the relevant memberships.

To remove a system role from an identity

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem roles**.
3. On the **System Roles** page, click the system role with a membership you want to delete.
4. In the **Edit System Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.
6. Next to the membership you want to delete, select the check box.
7. Click **Remove**.
8. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.

Managing my system roles' entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. Assigning identities to system roles avoids you having to assign entitlements separately to each identity. All a system role's entitlements are automatically assigned to all the identities assigned to the system role.

Detailed information about this topic

- [Displaying my system roles' entitlements](#) on page 298
- [Adding entitlements to my system roles](#) on page 298
- [Deleting my system roles' entitlements](#) on page 299

Displaying my system roles' entitlements

You can display entitlements that are assigned system roles for which you are responsible.

To display entitlements

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**System roles**.
3. On the **System Roles** page, click the system role whose entitlements you want to display.
4. In the **Edit System Role** pane, click the **Permissions** tab.

Adding entitlements to my system roles

You can add entitlements to system roles for which you are responsible. You do this through requests.

To add an entitlement to a system role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**System roles**.
3. On the **System Roles** page, click the system role to which you want to add an entitlement.
4. In the **Edit System Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.

9. Close the **Edit System Role** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.
After the request has been granted approval, the entitlement is added to the system role.

Related topics

- [Requesting products](#) on page 71

Deleting my system roles' entitlements

You can delete entitlements that are assigned system roles for which you are responsible.

To delete an entitlement of a system role

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities System roles**.
3. On the **System Roles** page, click the system role whose entitlements you want to delete.
4. In the **Edit System Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying my system roles' rule violations

You can display the rule violations of system roles for which you are responsible.

To display rule violations

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities System roles**.
3. On the **System Roles** page, click the system role whose rule violations you want to display.
4. On the **Edit System Role** pane, click the **Rule Violations** tab.

My system roles' history

The Web Portal allows you to display historical data of system roles for which you are responsible.

To do this, you have the following options:

Table 65: Historical data

View	Description
Events	Shows all events relating to the system role in table form (see Displaying my system roles' history on page 300).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of my system roles on page 300).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of my system roles on page 301).

Displaying my system roles' history

To track changes, you can display the history of system roles for which you are responsible.

To display the history

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **IdentitiesSystem roles**.
3. On the **System Roles** page, click the system role whose history you want to display.
4. In the **Edit System Role** pane, click the **History** tab.

Displaying the status overview of my system roles

You can display all the changes effecting system roles for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities System roles**.
3. On the **System Roles** page, click the system role whose status overview you want to display.
4. In the **Edit System Role** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of my system roles

You can compare the current status of a system role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click **Identities System roles**.
3. On the **System Roles** page, click the system role whose status you want to compare.
4. In the **Edit System Role** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Managing my assignment resources

Use assignment resources to request hierarchical roles, such as departments or business roles and assign them to identities, 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.

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 perform a variety of actions on the application roles that you manage and gather information about them.

Detailed information about this topic

- [Displaying my assignment resources](#) on page 302
- [Displaying and editing my assignment resource main data](#) on page 302

Displaying my assignment resources

You can display all the assignment resources for which you are responsible.

To display assignment resources

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Assignment resources**.
This opens the **Assignment resources** page and displays all the assignment resources for which you are responsible.
3. (Optional) To display details of an assignment resource, click the assignment resource.

Displaying and editing my assignment resource main data

You can display and edit the main data of the assignment resources for which you are responsible.

To display and edit an assignment resource's main data

1. In the menu bar, click **Responsibilities > My Responsibilities**.
2. In the navigation, click Identities**Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose main data you want to display/edit.
4. In the **Edit Assignment Resource** pane.

You can edit the following main data.

Table 66: Assignment resource main data

Property	Description
Assignment resource	Enter a full, descriptive name for the assignment resource.
Resource type	Select the resource type of the assignment resource. Use resource types to group assignment resources.
Description	Enter a full, descriptive name for the assignments resource.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning assignment resources to identities. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Product owner	Click Select/Change and then select an application role. The members of this application role can edit the main data of the assignment resource and be used as approvers in approval processes for assignment resource requests.

5. Click **Save**.

Managing task delegations

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

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

Role memberships and responsibilities can also be delegated to you.

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

Detailed information about this topic

- [Displaying delegations](#) on page 304
- [Creating delegations](#) on page 304
- [Canceling delegations](#) on page 305
- [Deleting delegations](#) on page 305

Displaying delegations

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

To display delegations

1. In the menu bar, click **Requests > Request history**.
2. On the **Request History** page, click **▼ (Filter)**.
3. In the filter context menu, select the **My delegations** check box.
4. (Optional) To display details of a delegation, click the corresponding delegation.

Creating delegations

You can delegate role memberships and responsibilities to other identities.

NOTE: You cannot edit a delegation afterward. If you want to make a change to the delegation, delete it (see [Deleting delegations](#) on page 305) and create a new delegation.

To create a delegation

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

- **The recipient can delegate this role:** (Optional) Select the check box to specify that the recipient can delegate their delegated role/responsibility on to another identity.
 - **Reason:** (Optional) In the dialog, enter a reason for the delegation.
 - **Priority:** (Optional) In the menu, select a priority for the delegation.
9. Click **Save**.

Canceling delegations

You can cancel delegations that you have already set up.

NOTE: You can only cancel delegations as long they have the **Request** or **Approved** status. You can delete delegations with the **Assigned** status (see [Deleting delegations](#) on page 305).

To cancel a delegation

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

Deleting delegations

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

NOTE: You can only delete delegations as long as they have the **Assigned** status. You can cancel delegations that have the **Request** or **Approved** status (see [Canceling delegations](#) on page 305).

To delete a delegation

1. In the menu bar, click **Requests > Request history**.
2. On the **Request History** page, click **▼ (Filter)**.
3. In the filter context menu, select the **My delegations** check box.
4. Click the delegation you want to delete.

5. In the **View Request Details** pane, click **Unsubscribe product**.
6. In the **Unsubscribe Product** pane, perform the following actions:
 - a. In the **Unsubscribed as from** field, specify the date on which to delete the delegation. If you leave this field empty, the delegation is deleted once you have clicked **Save**.
 - b. In the **Reason for your decision** field, enter a reason for your approval decision.
 - c. In the **Additional comments about your decision** field, enter extra information.
 - d. Click **Save**.

Ownerships

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

Detailed information about this topic

- [Assigning owners to system entitlements](#) on page 306
- [Assigning owners to devices](#) on page 307

Assigning owners to system entitlements

You can specify who is responsible for a system entitlement. To do this, you define a product owner for the service item that is assigned to the system entitlement. You can also take responsibility for system entitlement yourself.

To assign system entitlements to an owner

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

In the context of an attestation, the selected owner can confirm that this assignment is correct (see [Pending attestations](#) on page 136).

Related topics

- [Assigning owners to devices](#) on page 307

Assigning owners to devices

You can specify who is responsible for a device. To do this, you define a product owner for the service item that is assigned to the device. You can also take responsibility for the device yourself.

To assign an owner to a device

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

In the context of an attestation, the selected owner can confirm that this assignment is correct (see [Pending attestations](#) on page 136).

Related topics

- [Assigning owners to system entitlements](#) on page 306

Managing data

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

- Departments
- User accounts
- Business roles
- Identities
- Cost centers
- Multi-request resources
- Multi requestable/unsubscribable resources
- Resources
- Locations
- System entitlements
- System roles
- Assignment resources

Detailed information about this topic

- [Managing departments](#) on page 309
- [Managing user accounts](#) on page 324
- [Managing business roles](#) on page 327
- [Managing identities](#) on page 342
- [Managing cost centers](#) on page 361
- [Managing multi-request resources](#) on page 375
- [Managing multi requestable/unsubscribable resources](#) on page 377
- [Managing resources](#) on page 379
- [Managing locations](#) on page 381
- [Managing system entitlements](#) on page 395

- [Managing system roles](#) on page 414
- [Managing assignment resources](#) on page 423

Managing departments

You can use the Web Portal to manage departments.

Detailed information about this topic

- [Displaying departments](#) on page 309
- [Creating departments](#) on page 309
- [Copying/splitting departments](#) on page 314
- [Comparing and merging departments](#) on page 315
- [Restoring departments to their previous state](#) on page 316
- [Displaying and editing department main data](#) on page 312
- [Managing department memberships](#) on page 317
- [Managing department entitlements](#) on page 320
- [Displaying department rule violations](#) on page 322
- [Department history](#) on page 322
- [Restoring deleted departments](#) on page 324

Displaying departments

You can display any of the departments and their details.

To display departments

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **System roles**.
This opens the **Departments** page and displays all the departments.
3. (Optional) To display details of a department, click the department.

Creating departments

You can create new departments.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a department

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **System roles**.
3. On the **Departments** page click **+ Create department**.
4. In the **Create Department** pane, enter the main data of the department in the respective fields.

You can edit the following main data.

Table 67: Department main data

Property	Description
Department	Enter a full, descriptive name for the department.
Short name	Enter a short name for the department.
Object ID	Enter a unique object ID for the department. For example, the object ID is required in SAP systems for assigning identities to departments.
Parent department	Click Select/Change and select a department to be the parent department for organizing the department hierarchically. If you want the department at the root of a department hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the department.
Deputy manager	Select an identity to act as a deputy to the department's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Location	Click Select/Change and select the location the department is primarily assigned to.
Attestors	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the department.
Cost center	Click Select/Change and select the cost center the department is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the department.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the department.
Description	Enter a description for the department.

5. Click **Create**.

Displaying and editing department main data

You can display and edit departments' main data.

To display and edit a department's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **Departments**.
3. On the **Identities** page, click the department whose main data you want to display/edit.
4. In the **Edit Department** pane.

You can edit the following main data.

Table 68: Department main data

Property	Description
Department	Enter a full, descriptive name for the department.
Short name	Enter a short name for the department.
Object ID	Enter a unique object ID for the department. For example, the object ID is required in SAP systems for assigning identities to departments.
Parent department	Click Select/Change and select a department to be the parent department for organizing the department hierarchically. If you want the department at the root of a department hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the department.
Deputy manager	Select an identity to act as a deputy to the department's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Location	Click Select/Change and select the location the department is primarily assigned to.
Attestors	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the department.
Cost center	Click Select/Change and select the cost center the department is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the department.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the department.
Description	Enter a description for the department.

5. Click **Save**.

Copying/splitting departments

You can copy or move memberships and entitlements from departments you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a department or move memberships and entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page click the department you want to copy or whose memberships and entitlements you want to move.
4. In the **Edit Department** pane, click **⋮ (Actions)** > **Split**.
5. In the **Split** pane, in the **Type of new object** menu, select which type to give the new object.
6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

TIP: After the object has been created, you can add the remaining main data (see [Displaying and editing my department main data](#) on page 171, [Displaying and editing my business roles' main data](#) on page 202, [Displaying and editing my cost center main data](#) on page 236, or [Displaying and editing my locations' main data](#) on page 265).

7. Click **Next**.
8. In the **Select assignments to be copied or moved to the new object** step, perform the following actions:
 - To neither copy nor move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and do not copy or move to new object**. The entitlement/membership is later only available in the source object.
 - To copy or move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new object**. The entitlement/membership is included later in the source object as well as the target object.
 - To move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new object**. The entitlement/membership is later removed from the source object and only included in the target object.
9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.

Related topics

- [Managing department memberships](#) on page 317
- [Managing department entitlements](#) on page 320

Comparing and merging departments

You can compare properties of departments with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a department

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department you want to compare and merge.
4. In the **Edit Department** pane, click **⋮ (Actions) > Compare and merge**.
5. In the **Compare and Merge** pane, in the **Comparison object** field, click **Select**.
6. In the **Edit Property** pane, in the **Selected table** menu, select whether you want to compare and merge the department with a business role, department, cost center, or location.
7. Click the relevant business role, department, cost center, or location.
8. Click **Continue**.

The assigned memberships and entitlements of both objects are listed with the following information in the **View comparison result** step.

Table 69: Overview of the assignments

Column	Description
Assigned object	Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.

Column	Description
This object	<p>Shows you the assignment type of the entitlement/membership in the source or comparison object. The following assignment types are available.</p> <ul style="list-style-type: none"> • Direct • Inherited • Requested • Dynamic • Not assigned <p>For more detailed information about assigning company resources, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p>
Comparison object	

9. Click **Continue**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Merge**.

Related topics

- [Managing department memberships](#) on page 317
- [Managing department entitlements](#) on page 320

Restoring departments to their previous state

You can compare the current status of a department to its status at another time and completely or partially restore the historical state.

To restore a department to a previous state

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department you want to roll back.
4. In the **Edit Department** pane, click **⋮ (Actions) > Reset to previous state**.
5. In the **Reset to Previous State** pane, specify a date in the date field. This displays all changes that have taken place since the given date.
6. Select the check box next to the property that you want to restore to its previous state.

7. Click **Next**.
8. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
9. Click **Next**.

Related topics

- [Managing department memberships](#) on page 317
- [Managing department entitlements](#) on page 320

Managing department memberships

As soon as an identity is assigned to a department, the identity becomes a member in the department.

Detailed information about this topic

- [Displaying department memberships](#) on page 317
- [Analyzing assignments to departments](#) on page 318
- [Adding identities to departments](#) on page 318
- [Removing identities from departments](#) on page 320

Displaying department memberships

You can display which identities are assigned to certain departments.

To display memberships

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department whose memberships you want to display.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To view all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to departments

You can display how a department assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department whose memberships you want to display.
4. On the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click the membership to display its assignment analysis.

Adding identities to departments

You can add identities to departments.

The following assignment options are available:

- Assignment by [request](#)
- Automatic assignment through a [dynamic role](#)
- Revoking [exclusion](#) of a member

To assign an identity to a department using a request

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department to which you want to add an identity.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click **Request memberships**.
7. In the **Request Memberships** pane, next to the identity to which you want to assign the department, select the check box.
8. Click **Request memberships**.
9. Close the **Edit Department** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

Once the request has been granted approval, the identity is assigned to the department.

To add members automatically through a dynamic role

1. In the menu bar click **Data administration > Data Explorer**.
 2. In the Data Explorer navigation, click **Departments**.
 3. On the **Departments** page, click the department for which you want to create a dynamic role.
 4. In the **Edit Department** pane, click the **Memberships** tab.
 5. On the **Memberships** tab, click **Automatic memberships**.
 6. Click **Create dynamic role**.
 7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:
 - a. Click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition, click **Add another condition** and repeat the steps.
 - f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.
- TIP:** To remove a condition, click  (**Delete**).
- For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.
8. Click **Save**.
 9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.
 10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.
 11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department to which you want to re-add a member.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to re-add as a member.
7. Click **Remove exclusion**.

Related topics

- [Requesting products](#) on page 71

Removing identities from departments

You can remove identities from departments by deleting the corresponding memberships.

To remove a department from an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department that has a membership you want to delete.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.
6. Select the check box next to the membership you want to delete.
7. Click **Remove**.
8. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
9. Click **Delete memberships**.

TIP: If you only selected direct memberships, confirm the prompt in the **Remove Memberships** dialog with **Yes**.

Managing department entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to system roles you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the departments.

Detailed information about this topic

- [Displaying department entitlements](#) on page 321
- [Adding entitlements to departments](#) on page 321
- [Deleting department entitlements](#) on page 322

Displaying department entitlements

You can display entitlements assigned to departments.

To display entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department whose entitlements you want to display.
4. In the **Edit Department** pane, click the **Entitlements** tab.

Adding entitlements to departments

You can add entitlements to departments. You do this through a request.

To add an entitlement to a department

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department to which you want to add an entitlement.
4. In the **Edit Department** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.
9. Close the **Edit Department** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

After the request has been granted approval, the entitlement is added to the department.

Related topics

- [Requesting products](#) on page 71

Deleting department entitlements

You can delete entitlements assigned to departments.

To delete an entitlement from a department

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department whose entitlements you want to delete.
4. In the **Edit Department** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying department rule violations

You can display department rule violations.

To display rule violations

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department whose rule violations you want to display.
4. On the **Edit Department** pane, click the **Rule Violations** tab.

Department history

The Web Portal allows you to display historical data of departments.

To do this, you have the following options:

Table 70: Historical data

View	Description
Events	Shows all events relating to the department in table form (see Displaying department history on page 323).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of departments on page 323).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of departments on page 324).

Displaying department history

To track changes, you can display departments' history.

To display the history

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department whose history you want to display.
4. On the **Edit Department** pane, click the **History** tab.

Displaying the status overview of departments

You can display all the changes effecting departments for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department whose status overview you want to display.
4. In the **Edit Department** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of departments

You can compare the current status of a department that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click the department whose status you want to compare.
4. In the **Edit Department** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Restoring deleted departments

You can restore deleted departments. For example, a department can be deleted if two roles are merged (see [Comparing and merging departments](#) on page 315).

To restore a deleted department

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Departments**.
3. On the **Departments** page, click **Restore deleted object**.
4. In the **Restore Deleted Object** pane, click the department that you want to restore.
5. Click **Next**.
6. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
7. Click **Next**.

Managing user accounts

You can use the Web Portal to manage user accounts.

User accounts represent a target system's authentication objects. A user account obtains the required permissions for accessing target system resources through its memberships in groups and system entitlements.

A user account can be linked to an identity in One Identity Manager. However, you can also manage user accounts separately from identities.

Detailed information about this topic

- [Displaying user accounts](#) on page 325
- [Editing user accounts](#) on page 325
- [Displaying user account memberships](#) on page 326
- [Creating reports about user accounts](#) on page 326

Displaying user accounts

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

To display user accounts

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **System entitlements**.
This opens the **User accounts** page and displays all the user accounts.
3. (Optional) To control which user accounts are displayed, click **▼ (Filter)** (see [Filtering](#) on page 27). For example, this allows you to show just those user accounts that have no identity assigned to them.
4. (Optional) To display details of a user account, click the user account.

Editing user accounts

You can edit user accounts to assign identities to them, for example.

To edit a user account

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

Table 71: Service item main data

Property	Description
Identity	Select the identity to which the user account should be linked.

5. Click **Save**.

Managing user account memberships

As soon as a system entitlement is assigned to a user account, the user account becomes a member in the system entitlement.

Detailed information about this topic

- [Displaying user account memberships](#) on page 326

Displaying user account memberships

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

To display memberships

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **User accounts**.
3. On the **User Accounts** page, click the user account with the memberships you want to display.
4. In the **Edit User Account** pane, click the **Memberships** tab.

Creating reports about user accounts

You can create the following reports on user accounts:

- [Reports](#) on individual user accounts
- [Reports](#) on all user account of a specified target system

To create a report on a user account

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the data explorer, click **User accounts**.
3. On the **User Accounts** page, click the user account that you want to create a report on.
4. In the **Edit User Account**, click **Download report**.

To create a report on all user accounts of a specific target system

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the data explorer, click **User accounts**.
3. On the **User Accounts** page, click **Download target system report**.

4. In the **Download Target System Report** pane, click the target system with the user accounts you want to see in the report.
5. Click **Download report**.

Managing business roles

You can use the Web Portal to manage business roles.

Detailed information about this topic

- [Displaying business roles](#) on page 327
- [Creating business roles](#) on page 327
- [Displaying and editing business role main data](#) on page 330
- [Copying/splitting business roles](#) on page 332
- [Comparing and merging business roles](#) on page 333
- [Restoring business roles to their previous state](#) on page 334
- [Managing business role memberships](#) on page 335
- [Managing business role entitlements](#) on page 338
- [Displaying business role rule violations](#) on page 340
- [Business role history](#) on page 340
- [Restoring deleted business roles](#) on page 342

Displaying business roles

You can display any of the business roles and their details.

To display business roles

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Locations**.
This opens the **Business Roles** page and displays all the business roles.
3. (Optional) To display details of a business role, click the business role.

Creating business roles

You can create new business roles.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a business role

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Locations**.
3. On the **Business Roles** page, click **+ Create business role**.
4. In the **Create Business Role** pane, enter the main data of the business role in the respective fields.

You can edit the following main data.

Table 72: Business role main data

Property	Description
Business role	Enter a full, descriptive name for the business role.
Short name	Enter a short name for the business role.
Internal name	Enter a company internal name for the business role.
Description	Enter a description for the business role.
Role class	When you create the business role: Select the role class of the business role. To differentiate between different business roles, define company specific role classes. Role classes are used to specify which company resource assignments are possible through roles in a role class.
Parent business role	Click Select/Change and select a business role to be the parent business role for organizing the business role hierarchically. If you want the business role at the root of a business role hierarchy, leave the field empty.
Role type	Select the role type of the business role. Role types are mainly used to regulate approval policy inheritance.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the business role.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the business role.
Manager	Select the manager who is responsible for the business role.
Deputy manager	Select an identity to act as a deputy to the business role's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Identities do not inherit	Select this check box if you want to temporarily prevent identities from inheriting this business role.
Comment	Enter a comment for the business role.

5. Click **Create**.

Displaying and editing business role main data

You can display and edit the system roles' main data.

To display and edit a business role's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **Business roles**.
3. On the **Business Roles** page, click the business role whose main data you want to display/edit.
4. In the **Edit Business Role** pane.

You can edit the following main data.

Table 73: Business role main data

Property	Description
Business role	Enter a full, descriptive name for the business role.
Short name	Enter a short name for the business role.
Internal name	Enter a company internal name for the business role.
Description	Enter a description for the business role.
Role class	When you create the business role: Select the role class of the business role. To differentiate between different business roles, define company specific role classes. Role classes are used to specify which company resource assignments are possible through roles in a role class.
Parent business role	Click Select/Change and select a business role to be the parent business role for organizing the business role hierarchically. If you want the business role at the root of a business role hierarchy, leave the field empty.
Role type	Select the role type of the business role. Role types are mainly used to regulate approval policy inheritance.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the business role.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the business role.
Manager	Select the manager who is responsible for the business role.
Deputy manager	Select an identity to act as a deputy to the business role's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Identities do not inherit	Select this check box if you want to temporarily prevent identities from inheriting this business role.
Comment	Enter a comment for the business role.

5. Click **Save**.

Copying/splitting business roles

You can copy or move memberships and entitlements from business roles you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a business role or move memberships and entitlements

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role you want to copy or whose memberships and entitlements you want to move.
4. In the **Edit Business Role** pane, click **⋮ (Actions)** > **Split**.
5. In the **Split** pane, in the **Type of new object** menu, select which type to give the new object.
6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

TIP: After the object has been created, you can add the remaining main data (see [Displaying and editing my department main data](#) on page 171, [Displaying and editing my business roles' main data](#) on page 202, [Displaying and editing my cost center main data](#) on page 236, or [Displaying and editing my locations' main data](#) on page 265).

7. Click **Next**.
8. In the **Select assignments to be copied or moved to the new object** step, perform the following actions:
 - To neither copy nor move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and do not copy or move to new object**. The entitlement/membership is later only available in the source object.
 - To copy or move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new object**. The entitlement/membership is included later in the source object as well as the target object.
 - To move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new object**. The entitlement/membership is later removed from the source object and only included in the target object.
9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.

Related topics

- [Managing business role memberships](#) on page 335
- [Managing business role entitlements](#) on page 338

Comparing and merging business roles

You can compare properties of business roles with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a business role

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business roles** page, click the business role that you want to compare and merge.
4. In the **Edit Business Role** pane, click **⋮ (Actions)** > **Compare and merge**.
5. In the **Compare and Merge** pane, in the **Comparison object** field, click **Select**.
6. In the **Edit Property** pane, in the **Selected table** menu, select whether you want to compare and merge the business role with a business role, department, cost center, or location.
7. Click the relevant business role, department, cost center, or location.
8. Click **Continue**.

The assigned memberships and entitlements of both objects are listed with the following information in the **View comparison result** step.

Table 74: Overview of the assignments

Column	Description
Assigned object	Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.

Column	Description
This object	<p>Shows you the assignment type of the entitlement/membership in the source or comparison object. The following assignment types are available.</p> <ul style="list-style-type: none"> • Direct • Inherited • Requested • Dynamic • Not assigned <p>For more detailed information about assigning company resources, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p>
Comparison object	

9. Click **Continue**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Merge**.

Related topics

- [Managing business role memberships](#) on page 335
- [Managing business role entitlements](#) on page 338

Restoring business roles to their previous state

You can compare the current state of a business role to its state at another time and completely or partially restore the historical state.

To restore a business role to a previous state

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role you want to roll back.
4. In the **Edit Business Role** pane, click **⋮ (Actions) > Reset to previous state**.
5. In the **Reset to Previous State** pane, specify a date in the date field. This displays all changes that have taken place since the given date.
6. Select the check box next to the property that you want to restore to its previous state.

7. Click **Next**.
8. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
9. Click **Next**.

Related topics

- [Managing business role memberships](#) on page 335
- [Managing business role entitlements](#) on page 338

Managing business role memberships

As soon as a business role is assigned to an identity, the identity becomes a member in the business role.

Detailed information about this topic

- [Displaying business role memberships](#) on page 335
- [Analyzing assignments to business roles](#) on page 336
- [Assigning identities to business roles](#) on page 336
- [Removing business roles from identities](#) on page 338

Displaying business role memberships

You can display which identities are assigned to certain business roles.

To display memberships

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role whose memberships you want to display.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To view all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to business roles

You can display how a business role assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role whose memberships you want to display.
4. On the **Edit Business Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click the membership to display its assignment analysis.

Assigning identities to business roles

You can assign business roles to identities.

The following assignment options are available:

- Assignment by [request](#)
- Automatic assignment through a [dynamic role](#)
- Revoking [exclusion](#) of a member

To assign an identity to a business role using a request

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business roles** page, click the business role to which you want to assign an identity.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click **Request memberships**.
7. In the **Request Memberships** pane, next to the identity to which you want to assign the business role, select the check box.
8. Click **Request memberships**.
9. Close the **Edit Business Role** pane.
10. In the menu bar, click **Requests** > **Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

Once the request has been granted approval, the identity is assigned to the business role.

To add members automatically through a dynamic role

1. In the menu bar click **Data administration > Data Explorer**.
 2. In the Data Explorer navigation, click **Business roles**.
 3. On the **Business Roles** page, click the business role for which you want to create a dynamic role.
 4. In the **Edit Business Role** pane, click the **Memberships** tab.
 5. On the **Memberships** tab, click **Automatic memberships**.
 6. Click **Create dynamic role**.
 7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:
 - a. Click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition, click **Add another condition** and repeat the steps.
 - f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.
- TIP:** To remove a condition, click  (**Delete**).
- For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.
8. Click **Save**.
 9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.
 10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.
 11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role to which you want to re-add a member.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to re-add as a member.
7. Click **Remove exclusion**.

Related topics

- [Requesting products](#) on page 71

Removing business roles from identities

You can remove identities from business roles by deleting the corresponding memberships.

To remove a business role from an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role that has a membership you want to delete.
4. In the **Edit Business Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.
6. Select the check box next to the membership you want to delete.
7. Click **Remove**.
8. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
9. Click **Delete memberships**.

TIP: If you only selected direct memberships, confirm the prompt in the **Remove Memberships** dialog with **Yes**.

Managing business role entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. Assigning identities to business roles avoids you having to assign entitlements separately to each identity. All a business role's entitlements are automatically assigned to all the identities assigned to the business role.

Detailed information about this topic

- [Displaying business role entitlements](#) on page 339
- [Adding entitlements to business roles](#) on page 339
- [Deleting business role entitlements](#) on page 340

Displaying business role entitlements

You can display entitlements assigned to business roles.

To display entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role whose entitlements you want to display.
4. In the **Edit Business Role** pane, click the **Entitlements** tab.

Adding entitlements to business roles

You can add entitlements to business roles. You do this through a request.

To add an entitlement to a business role

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role to which you want to add an entitlement.
4. In the **Edit Business Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.
9. Close the **Edit Business Role** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

After the request has been granted approval, the entitlement is added to the business role.

Related topics

- [Requesting products](#) on page 71

Deleting business role entitlements

You can delete entitlements assigned to business roles.

To delete an entitlement from a business role

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role whose entitlements you want to delete.
4. In the **Edit Business Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying business role rule violations

You can display business role rule violations.

To display rule violations

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role whose rule violations you want to display.
4. On the **Edit Business Role** pane, click the **Rule Violations** tab.

Business role history

The Web Portal allows you to display historical data of business roles.

To do this, you have the following options:

Table 75: Historical data

View	Description
Events	Shows all events relating to the business role in table form (see Displaying business role history on page 341).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of business roles on page 341).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of business roles on page 342).

Displaying business role history

To track changes, you can display business roles' history.

To display the history

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role whose history you want to display.
4. On the **Edit Business Role** pane, click the **History** tab.

Displaying the status overview of business roles

You can display all the changes effecting business roles for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role whose status overview you want to display.
4. In the **Edit Business Role** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of business roles

You can compare the current status of a business role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business Roles** page, click the business role whose status you want to compare.
4. In the **Edit Business Role** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Restoring deleted business roles

You can restore deleted business roles. For example, a business role can be deleted if two roles are merged (see [Comparing and merging business roles](#) on page 333).

To restore a deleted business role

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Business roles**.
3. On the **Business roles** page, click **Restore deleted object**.
4. In the **Restore Deleted Object** pane, click the business role that you want to restore.
5. Click **Next**.
6. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
7. Click **Next**.

Managing identities

You can use the Web Portal to manage identities.

Detailed information about this topic

- [Displaying identities](#) on page 343
- [Displaying and editing identity main data](#) on page 343
- [Creating identities](#) on page 345
- [Comparing identities](#) on page 348
- [Displaying and analyzing identities' risk indexes](#) on page 349
- [Deactivating identities](#) on page 350
- [Reactivating identities](#) on page 350
- [Marking identities as security risks](#) on page 350
- [Deleting identities](#) on page 351
- [Assigning other managers to identities](#) on page 352
- [Creating reports about identities](#) on page 352
- [Managing identities' memberships](#) on page 353
- [Displaying identities' organizational charts](#) on page 357
- [Identity history](#) on page 357
- [Managing attestation cases of identities](#) on page 359
- [Displaying identities' rule violations](#) on page 361

Displaying identities

You can display any of the identities and their details.

To display identities

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the navigation, click **Identities**.
This opens the **Identities** page and displays all the identities.
3. (Optional) To display details of an identity, click the identity.

Displaying and editing identity main data

You can display and edit identities' main data.

To display and edit an identity's main data

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

3. On the **Identities** page, click the identity whose main data you want to display/edit.
4. In the **Edit Identity** pane, expand the one of the sections.
5. Make your changes in the corresponding fields:

You can edit the following main data.

Table 76: Identities main data

Property	Description
Personal data	
Last name	Enter the identity's last name.
First name	Enter the identity's first name.
Middle name	Enter the identity's middle name.
Date of birth	Enter the identity's date of birth. Click the  (Calendar) to do this and use the date picker to select the date of birth.
Personnel number	Enter the identity's personnel number.
Gender	In the menu, select the identity's gender.
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Resetting the password through the help desk is permitted.	Select the check box to allow password help desk staff to reset the identity's password in the Operations Support Web Portal.
Identity does not pose a security risk/Identity poses a security risk	Toggle the switch to specify whether the identity poses a security risk or not (see Marking my identities as security risks on page 223).
Organizational information	
Primary cost center	Click Select/Change and select the identity's primary cost center.
Primary department	Click Select/Change and select the identity's primary department.
External	Select the check box if this is an external identity.
Employee type	In the menu, select what type of identity this is. For example, an identity of this company or a trainee.
Entry date	Enter the date the identity started at the company. Click the  (Calendar) and use the date picker to select the starting date.

Property	Description
Leaving date	Enter the date that the identity leaves the company. Click the  (Calendar) to do this and use the date picker to select the leaving date.
Manager	Shows you the identity's manager. TIP: If necessary, you can transfer the identity's manager at a later date (see Assigning other managers to my identities on page 224).
Permanently deactivated	Select the check box if you want the identity to be permanently deactivated (see Deactivating my identities on page 222).
Temporarily disabled	Select the check box if you want to deactivate the identity only temporarily.
Location information	
Primary location	Click Select/Change and select the identity's primary location.
Building	Enter the building where the identity works.
Floor	Enter which floor the identity works on.
Room	Enter the room the identity works in.
Street	Enter the street or road where the identity works.
Zip code	Enter the zip code of the identity's work location.
City	Enter the city where the identity works.
Country	In the menu, select the country where the identity works.
State	In the menu, select the state where the identity works.

6. Click **Save**.

Creating identities

You can add new identities. This function is mainly designed for adding external identities. For example, subcontractors who are not entered in the human resources department. Data from new identities 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.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Identities**.
3. On the **Identities** page, click **+ Create identity**.
4. In the **Create Identity** pane, enter the main data of the identity in the respective fields.

You can edit the following main data.

Table 77: Identities main data

Property	Description
Unique data	
First name	Enter the identity's first name.
Last name	Enter the identity's last name.
Central user account	Enter the name of the identity's central user account.
Default email address	Enter the identity's default email address.
Personal data	
Second name	Enter the identity's middle name.
Date of birth	Enter the identity's date of birth. Click the  (Calendar) to do this and use the date picker to select the date of birth.
Personnel number	Enter the identity's personnel number.
Gender	In the menu, select the identity's gender.
Resetting the password through the help desk is permitted.	Select the check box to allow password help desk staff to reset the identity's password in the Operations Support Web Portal.
Organizational information	
Primary cost center	Click Select/Change and select the identity's primary cost center.
Primary department	Click Select/Change and select the identity's primary department.
External	Select the check box if this is an external identity.
Identity	Select the identity type of the identity: <ul style="list-style-type: none">• Primary identity: Default identity for an identity. The identity has a default user account.

Property	Description
	<ul style="list-style-type: none"> • Organizational identity: Virtual identity (sub identity) for mapping different roles of an identity within the organization. The sub identity is associated with a user account of the Organizational identity type. In addition, specify a main identity. • Personal administrator identity: Virtual identity (sub identity) associated with a user account of type Personal administrator identity type. In addition, specify a main identity. • Sponsored identity: Pseudo identity associated with a user account of type Sponsored identity. Also assign a manager to the identity. • Shared identity: Pseudo identity associated with an administrative user account of type Shared identity. Also assign a manager to the identity. • Service identity: Pseudo identity associated with a user account of type Service identity. Also assign a manager to the identity. • Machine identity: Pseudo identity for mapping machine identities. <p>For more information about mapping multiple identities of one identity, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p>
Employee type	In the menu, select what type of identity this is. For example, an identity of this company or a trainee.
Entry date	Enter the date the identity started at the company. Click the  (Calendar) and use the date picker to select the starting date.
Leaving date	Enter the date that the identity leaves the company. Click the  (Calendar) to do this and use the date picker to select the leaving date.
Manager	Shows you the identity's manager. TIP: If necessary, you can transfer the identity's manager at a later date (see Assigning other managers to my identities on page 224).
Permanently deactivated	Select the check box if you want the identity to be permanently deactivated (see Deactivating my identities on page 222).

Property	Description
Temporarily disabled	Select the check box to activate the identity at a later date then click the  (Calendar) and use the date picker to select the date to activate the identity.
Details of the location.	
Primary location	Click Select/Change and select the identity's primary location.
Building	Enter the building where the identity works.
Floor	Enter which floor the identity works on.
Room	Enter the room the identity works in.
Street	Enter the street or road where the identity works.
Zip code	Enter the zip code of the identity's work location.
City	Enter the city where the identity works.
Country	In the menu, select the country where the identity works.
State	In the menu, select the state where the identity works.

The Web Portal checks whether identities with certain identical properties already exist.

- (Optional) Depending on the result of the check, you can display identities with identical properties and adjust the main data of the identities if necessary.
- Click **Create**.

Saving then checks again whether identities with certain identical properties already exist.

- (Optional) If the check finds an identity with identical properties, perform one of the following actions:
 - To create the identity, in the **Create Identity with Same Properties** dialog, click **Yes**.
 - To edit the identity and its properties before creating it, in the **Create Identity with Same Properties** dialog, click **No** and edit the main data of the identity you want to create.

Comparing identities

You can compare departments with each other. For example, you can identify missing entitlements for individual identities so that they can be requested again in a targeted manner.

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click **⋮ (Actions) > Compare identities**.
4. In the **Specify Parameters** pane, perform the following actions:
 - a. In the **Identities to compare** field, click **Select**.
 - b. In the **Edit Property** pane, select the check boxes next to the identities you want to compare.
 - c. Click **Apply**.
5. (Optional) To specify how to mark the similarities, in the **Specify Parameters** pane, perform the following actions:
 - a. In the **Lower bound [%] yellow** field, specify the percentage of similarity required before properties are highlighted in yellow. For example, if you enter a value of **70** here, all the properties that have a similarity of 70% or more will be marked in orange.
 - b. In the **Lower bound [%] orange**, specify the percentage of similarity required before properties are highlighted in orange. For example, if you enter the value **50** here, then all properties that have a similarity of 50% or more will be marked in orange.
6. (Optional) To specify which object types to include in the comparison, perform the following actions:
 - a. In the **Select object types** field, click **Select**.
 - b. In the **Edit Property** pane, select the check boxes next to the object types you want to take into account.
 - c. Click **Apply**.
7. Click **Show report**.

Displaying and analyzing identities' risk indexes

You can display identities' risk indexes and analyze how they are put together.

NOTE: For more detailed information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

To display and analyze an identity's risk index

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose risk index you want to display

and analyze.

4. In the **Edit Identity** pane, click **⋮ (Actions) > Analyze risk**.

Deactivating identities

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

Effects of permanent deactivating an identity are:

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

To deactivate an identity

1. On the **Identities** page, click the identity you want to deactivate.
2. Click **Save**.

Reactivating identities

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

To reactivate an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity you want to activate.
4. In the **Edit Identity** pane, toggle the switch next to **Identity is inactive**.
The text next to the switch changes to **Identity is active**.
5. Click **Save**.

Marking identities as security risks

You can mark identities as a security risk. Then the user accounts and resources of the affected identity are locked.

To mark an identity as a security risk

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity you want to mark as a security risk.
4. In the **Edit Identity** pane, toggle the switch next to **Identity poses a security risk**.
5. In the **Mark Identity as Security Risk** dialog, confirm the prompt with **Yes**.
The text next to the switch changes to **Identity poses a security risk**.
6. Click **Save**.

Revoking identities' security risks

If identities have been marked as a security risk, you can unmark them again. Then the affected identity regains access to user accounts and resources.

To revoke an identity's security risk

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click .
3. On the **Identities** page, click the relevant identity.
4. In the **Edit Identity** pane, toggle the switch next to **Identity poses a security risk**.
5. In the **Resolve Security Risk** dialog, confirm the prompt with **Yes**.
The text next to the switch changes to **Identity does not pose a security risk**.
6. Click **Save**.

Related topics

- [Displaying and editing identity main data](#) on page 343

Deleting identities

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

To delete an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity you want to delete.
4. In the **Edit Identity Data** area, click **Delete**.
5. In the **Delete Identity** dialog, confirm the prompt with **Yes**.

Assigning other managers to identities

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

To assign a manager to an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity that you want to assign to a new manager.
4. In the **Edit Identity** pane, click in the **Manager** field to select the manager you want to assign to the identity.

TIP: To remove the current manager, in the **Manager** menu, click **✕ (Remove assignment)**.

5. Click **Save**.

Creating reports about identities

You can create the following reports on identities:

- [Reports](#) on individual identities
- [Reports](#) on a specific identity that reports directly to you
- [Reports](#) on all identities that report directly to you
- [Reports](#) on rule violations that report directly to you.
- [Reports](#) on user accounts assigned to identities that report directly to you

To create a report on an individual identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity that you want to create a report on.
4. In the **Edit Identity**, click **⋮ (Actions) > Download report**.

To create a report about identities that report to a specific identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity to create a report on the identities who report directly to them.
4. In the **Edit Identity** section, click **⋮ (Actions) > Download report on identities who report directly to this identity**.

To create a report on all identities that report directly to you

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click **⋮ (Actions) > Download report on identities who report directly to you**.

To create a report on rule violations by identities that report directly to you

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click **⋮ (Actions) > Download report on rule violations by identities who report directly to you**.

To create a report on user accounts assigned to identities that report directly to you

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click **⋮ (Actions) > Download report on user accounts of identities who report directly to you**.

Managing identities' memberships

Identity assignments to company structures and entitlements are enabled through membership in the respective company structures. For example, if an identity is going to be assigned to a particular department, it must first have membership in that department.

Detailed information about this topic

- [Analyzing identities' membership assignments](#) on page 354
- [Displaying identities' departments](#) on page 354
- [Displaying identities' application roles](#) on page 354
- [Displaying identities' user accounts](#) on page 355

- [Displaying identities' business roles](#) on page 355
- [Displaying identities' cost centers](#) on page 355
- [Displaying identities' shops](#) on page 356
- [Displaying identities' locations](#) on page 356
- [Displaying identities' system entitlements](#) on page 356
- [Displaying identities' system roles](#) on page 357

Analyzing identities' membership assignments

You can see how an identity membership came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **User accounts**.
3. On the **Identities** page, click the identity whose memberships you want to display.
4. On the **Edit Identity** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click the appropriate object types (for example, departments) in the navigation.
6. Click the membership to display its assignment analysis.

Displaying identities' departments

You can display departments that are assigned identities.

To display an identity's departments

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity whose departments you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Departments**.

Displaying identities' application roles

You can display application roles assigned to identities.

To display an identity's application roles

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity whose application roles you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Application roles**.

Displaying identities' user accounts

You can display user accounts assigned to identities.

To display an identity's user accounts

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity whose user accounts you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **User accounts**.

Displaying identities' business roles

You can display business roles that are assigned identities.

To display an identity's business roles

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity whose business roles you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Business roles**.

Displaying identities' cost centers

You can display cost centers that are assigned identities.

To display an identity's cost centers

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity whose cost centers you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Cost centers**.

Displaying identities' shops

You can display shops that are assigned identities.

To display an identity's shops

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity whose shops you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Shops**.

Displaying identities' locations

You can display locations that are assigned identities.

To display an identity's locations

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity whose locations you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **Locations**.

Displaying identities' system entitlements

You can display system entitlements assigned to identities.

To display an identity's system entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.

3. On the **Identities** page, click the identity whose system entitlements you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **System entitlements**.

Displaying identities' system roles

You can display system roles that are assigned identities.

To display an identity's system roles

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **Identities**.
3. On the **Identities** page, click the identity whose system roles you want to display.
4. In the **Edit Identity** pane, click the **Memberships** tab.
5. In the navigation on the **Memberships** tab, click **System roles**.

Displaying identities' organizational charts

You can display identities' organizational charts.

To display an identity's organizational chart

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose organizational charts you want to display.
4. In the **Edit Identity** pane, click the **Organizational Chart** tab.

Identity history

The Web Portal allows you to display historical data of identities.

To do this, you have the following options:

Table 78: Historical data

View	Description
Events	Shows all events relating to the identity in table form (see Displaying identities' history on page 358).

View	Description
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of identities on page 358).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of identities on page 359).

Displaying identities' history

To track changes, you can display identities' history.

To display the history

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **User accounts**.
3. On the **Identities** page, click the identity whose history you want to display.
4. On the **Edit Identity** pane, click the **History** tab.

Displaying the status overview of identities

You can display all the changes effecting identities for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **User accounts**.
3. On the **Identities** page, click the identity whose status overview you want to display.
4. In the **Edit Identity** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of identities

You can compare the current status of an identity that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **User accounts**.
3. On the **Identities** page, click the identity whose status you want to compare.
4. In the **Edit Identity** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Managing attestation cases of identities

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

Detailed information about this topic

- [Displaying attestation cases of identities](#) on page 359
- [Approving and denying attestation cases of identities](#) on page 360

Displaying attestation cases of identities

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

To display attestation cases of an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. In the **Edit Identity** pane, click the **Attestation** tab.
This displays all the identity's attestation cases.
5. (Optional) To display more details of an attestation case, click the corresponding attestation case.

Related topics

- [Attestation](#) on page 113
- [Displaying pending attestation cases](#) on page 137

Approving and denying attestation cases of identities

You can make an approval decision about certain identity attestation cases (approve or deny).

To approve an attestation case

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose attestation cases you want decide.
4. In the **Edit Identity** pane, click the **Attestation** tab.
5. On the **Attestation** tab, click ▼ (**Filter**).
6. In the filter context menu, under **State**, select the **Pending** option.
7. Perform one of the following actions:
 - To approve an attestation case, select the check box next to the attestation case in the list and click **Approve** below the list.
 - To deny an attestation case, select the check box next to the attestation case in the list and click **Deny** below the list.
8. (Optional) In the **Approve Attestation Case** or the **Deny Attestation Case** pane, perform the following actions:
 - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
 - b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

9. Click **Save**.

Related topics

- [Attestation](#) on page 113
- [Approving or denying attestation cases](#) on page 138

Displaying identities' rule violations

You can display the rule violations of identities.

You can also display mitigating controls for each rule violation.

To display identities' rule violations

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity whose rule violations you want to display.
4. In the **Edit Identity** pane, click the **Rule Violations** tab.
5. (Optional) To display the mitigating controls of a rule violation, click **View mitigating controls** next to the rule violation.

Related topics

- [Displaying compliance rules](#) on page 152

Managing cost centers

You can use the Web Portal to manage cost centers.

Detailed information about this topic

- [Displaying cost centers](#) on page 362
- [Creating cost centers](#) on page 362
- [Displaying and editing cost center main data](#) on page 363
- [Copying/splitting cost centers](#) on page 365
- [Comparing and merging cost centers](#) on page 366
- [Restoring cost centers to their previous state](#) on page 367
- [Managing cost center memberships](#) on page 368
- [Managing cost center entitlements](#) on page 371
- [Displaying cost center rule violations](#) on page 373
- [Cost center history](#) on page 373
- [Restoring deleted cost centers](#) on page 375

Displaying cost centers

You can display any of the cost centers and their details.

To display cost centers

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Cost centers**.
This opens the **Cost centers** page and displays all the cost centers.
3. (Optional) To display details of a cost center, click the cost center.

Creating cost centers

You can create new cost centers

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a cost center

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Cost centers**.
3. On the **Cost Centers** page, click **+ Create cost center**.
4. In the **Create Cost Center** pane, enter the main data of the cost center in the respective fields.

You can edit the following main data.

Table 79: Cost center main data

Property	Description
Cost center	Enter a full, descriptive name for the cost center.
Short name	Enter a short name for the cost center.
Parent cost center	Click Select/Change and select a cost center to be the parent cost center for organizing the cost center hierarchically. If you want the cost center at the root of a cost center hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the cost center.
Deputy manager	Select an identity to act as a deputy to the cost center's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Attestors	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the cost center.
Department	Click Select/Change and select the department the cost center is primarily assigned to.
Location	Click Select/Change and select the location the cost center is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the cost center.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the cost center.
Description	Enter a description for the cost center.

5. Click **Create**.

Displaying and editing cost center main data

You can display and edit cost centers' main data.

To display and edit a cost center's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **Cost centers**.
3. On the **Cost Centers** page, click the cost centers whose main data you want to display/edit.
4. In the **Edit Cost Center** pane.

You can edit the following main data.

Table 80: Cost center main data

Property	Description
Cost center	Enter a full, descriptive name for the cost center.
Short name	Enter a short name for the cost center.
Parent cost center	Click Select/Change and select a cost center to be the parent cost center for organizing the cost center hierarchically. If you want the cost center at the root of a cost center hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the cost center.
Deputy manager	Select an identity to act as a deputy to the cost center's manager.
Additional managers	Click Select/Change and select an application role. Members of the selected application role are responsible for the department.
Attestors	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the cost center.
Department	Click Select/Change and select the department the cost center is primarily assigned to.
Location	Click Select/Change and select the location the cost center is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the cost center.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the cost center.
Description	Enter a description for the cost center.

5. Click **Save**.

Copying/splitting cost centers

You can copy or move memberships and entitlements from cost centers you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a cost center or move memberships and entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center you want to copy or whose memberships and entitlements you want to move.
4. In the **Edit Cost Center** pane, click **⋮ (Actions) > Split**.
5. In the **Split** pane, in the **Type of new object** menu, select which type to give the new object.
6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

TIP: After the object has been created, you can add the remaining main data (see [Displaying and editing my department main data](#) on page 171, [Displaying and editing my business roles' main data](#) on page 202, [Displaying and editing my cost center main data](#) on page 236, or [Displaying and editing my locations' main data](#) on page 265).

7. Click **Next**.
8. In the **Select assignments to be copied or moved to the new object** step, perform the following actions:
 - To neither copy nor move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and do not copy or move to new object**. The entitlement/membership is later only available in the source object.
 - To copy or move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new object**. The entitlement/membership is included later in the source object as well as the target object.
 - To move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new object**. The entitlement/membership is later removed from the source object and only included in the target object.
9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.

Related topics

- [Managing cost center memberships](#) on page 368
- [Managing cost center entitlements](#) on page 371

Comparing and merging cost centers

You can compare properties of cost centers with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a cost center

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center you want to compare and merge.
4. In the **Edit Cost Center** pane, click **⋮ (Actions) > Compare and merge**.
5. In the **Compare and Merge** pane, in the **Comparison object** field, click **Select**.
6. In the **Edit Property** pane, in the **Selected table** menu, select whether you want to compare and merge the cost center with a business role, department, cost center, or location.
7. Click the relevant business role, department, cost center, or location.
8. Click **Continue**.

The assigned memberships and entitlements of both objects are listed with the following information in the **View comparison result** step.

Table 81: Overview of the assignments

Column	Description
Assigned object	Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.

Column	Description
This object	<p>Shows you the assignment type of the entitlement/membership in the source or comparison object. The following assignment types are available.</p> <ul style="list-style-type: none"> • Direct • Inherited • Requested • Dynamic • Not assigned <p>For more detailed information about assigning company resources, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p>
Comparison object	

9. Click **Continue**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Merge**.

Related topics

- [Managing cost center memberships](#) on page 368
- [Managing cost center entitlements](#) on page 371

Restoring cost centers to their previous state

You can compare the current state of a cost center to its state at another time and completely or partially restore the historical state.

To restore a cost center to a previous state

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center you want to roll back.
4. In the **Edit Cost Center** pane, click **⋮ (Actions) > Reset to previous state**.
5. In the **Reset to Previous State** pane, specify a date in the date field. This displays all changes that have taken place since the given date.
6. Select the check box next to the property that you want to restore to its previous state.

7. Click **Next**.
8. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
9. Click **Next**.

Related topics

- [Managing cost center memberships](#) on page 368
- [Managing cost center entitlements](#) on page 371

Managing cost center memberships

As soon as an identity is assigned to a cost center, the identity becomes a member in the cost center.

Detailed information about this topic

- [Displaying cost center memberships](#) on page 368
- [Analyzing assignments to cost centers](#) on page 369
- [Adding identities to cost centers](#) on page 369
- [Removing identities from cost centers](#) on page 371

Displaying cost center memberships

You can display which identities are assigned to certain cost centers.

To display memberships

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose memberships you want to display.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To view all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to cost centers

You can display how a cost center assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose memberships you want to display.
4. On the **Edit Cost Center** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click the membership to display its assignment analysis.

Adding identities to cost centers

You can add identities to cost centers.

The following assignment options are available:

- Assignment by [request](#)
- Automatic assignment through a [dynamic role](#)
- Revoking [exclusion](#) of a member

To assign an identity to a cost center using a request

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center to which you want to add an identity.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click **Request memberships**.
7. In the **Request Memberships** pane, next to the identity to which you want to assign the cost center, select the check box.
8. Click **Request memberships**.
9. Close the **Edit Cost Center** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

Once the request has been granted approval, the identity is assigned to the cost center.

To add members automatically through a dynamic role

1. In the menu bar click **Data administration > Data Explorer**.
 2. In the Data Explorer navigation, click **Cost centers**.
 3. On the **Cost centers** page, click the cost center for which you want to create a dynamic role.
 4. In the **Edit Cost Center** pane, click the **Memberships** tab.
 5. On the **Memberships** tab, click **Automatic memberships**.
 6. Click **Create dynamic role**.
 7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:
 - a. Click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition, click **Add another condition** and repeat the steps.
 - f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.
- TIP:** To remove a condition, click  (**Delete**).
- For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.
8. Click **Save**.
 9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.
 10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.
 11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center to which you want to re-add a member.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.

6. Select the check box next to the identity you want to re-add as a member.
7. Click **Remove exclusion**.

Related topics

- [Requesting products](#) on page 71

Removing identities from cost centers

You can remove identities from cost centers by deleting the corresponding memberships.

To remove a cost center from an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center that has a membership you want to delete.
4. In the **Edit Cost Center** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.
6. Select the check box next to the membership you want to delete.
7. Click **Remove**.
8. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
9. Click **Delete memberships**.

TIP: If you only selected direct memberships, confirm the prompt in the **Remove Memberships** dialog with **Yes**.

Managing cost center entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to cost centers you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the cost centers.

Detailed information about this topic

- [Displaying cost center entitlements](#) on page 372
- [Adding entitlements to cost centers](#) on page 372
- [Deleting cost center entitlements](#) on page 373

Displaying cost center entitlements

You can display entitlements assigned to cost centers.

To display entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose entitlements you want to display.
4. In the **Edit Cost Center** pane, click the **Entitlements** tab.

Adding entitlements to cost centers

You can add entitlements to cost centers. You do this through a request.

To add an entitlement to a cost center

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center to which you want to add an entitlement.
4. In the **Edit Cost Center** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.
9. Close the **Edit Cost Center** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

After the request has been granted approval, the entitlement is added to the cost center.

Related topics

- [Requesting products](#) on page 71

Deleting cost center entitlements

You can delete entitlements assigned to cost centers.

To delete an entitlement from a cost center

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose entitlements you want to delete.
4. In the **Edit Cost Center** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying cost center rule violations

You can display cost center rule violations.

To display rule violations

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose rule violations you want to display.
4. On the **Edit Cost Center** pane, click the **Rule Violations** tab.

Cost center history

The Web Portal allows you to display historical data of cost centers.

To do this, you have the following options:

Table 82: Historical data

View	Description
Events	Shows all events relating to the cost center in table form (see Displaying cost center history on page 374).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of cost centers on page 374).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of cost centers on page 375).

Displaying cost center history

To track changes, you can display cost centers' history.

To display the history

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose history you want to display.
4. On the **Edit Cost Center** pane, click the **History** tab.

Displaying the status overview of cost centers

You can display all the changes effecting cost centers for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose status overview you want to display.
4. In the **Edit Cost Center** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of cost centers

You can compare the current status of a cost center that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost Centers** page, click the cost center whose status you want to compare.
4. In the **Edit Cost Center** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Restoring deleted cost centers

You can restore deleted cost centers. For example, a cost center can be deleted if two roles are merged (see [Comparing and merging cost centers](#) on page 366).

To restore a deleted cost center

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Cost centers**.
3. On the **Cost centers** page, click **Restore deleted object**.
4. In the **Restore Deleted Object** pane, click the cost center that you want to restore.
5. Click **Next**.
6. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
7. Click **Next**.

Managing multi-request resources

You can use the Web Portal to manage multi-request resources.

Detailed information about this topic

- [Displaying multi-request resources](#) on page 376
- [Displaying and editing multi-request resources main data](#) on page 376

Displaying multi-request resources

You can display any of the requestable resources and their details.

To display multi-request resources

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Multi-request resources**.
This opens the **Multi-request Resources** page and displays all the multi-request resources.
3. (Optional) To display details of a multi-request resource, click the multi-request resource.

Displaying and editing multi-request resources main data

You can display and edit multi-request resources' main data.

To display and edit a multi-request resource's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **Multi-request resources**.
3. On the **Multi-request Resources** page, click the multi-request resource whose main data you want to display/edit.
4. In the **Edit Multi-Request Resource** pane.

You can edit the following main data.

Table 83: Multi-request resource main data

Property	Description
Multi-request resource	Enter a full, descriptive name for the multi-request resource.
Resource type	Select the resource type of the multi-request resource. Use resource types to group multi-request resources.
Description	Enter a description for the multi-request resource.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning multi-request resources to identities. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Product owner	Click Select/Change and then select an application role. The members of this application role can edit the main data of the multi-request resource and be used as approvers in approval processes for multi-request resource requests.

5. Click **Save**.

Managing multi requestable/unsubscribable resources

You can use the Web Portal to manage multi requestable/unsubscribable resources.

Detailed information about this topic

- [Displaying multi requestable/unsubscribable resources](#) on page 377
- [Displaying and editing multi requestable/unsubscribable resource main data](#) on page 378

Displaying multi requestable/unsubscribable resources

You can display any of the multi requestable/unsubscribable resources and their details.

To display multi requestable/unsubscribable resources

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Multi requestable/unsubscribable resources**.
This opens the **Multi requestable/unsubscribable Resources** page and displays all the multi requestable/unsubscribable resources.
3. (Optional) To display details of a multi requestable/unsubscribable resource, click the multi requestable/unsubscribable resource.

Displaying and editing multi requestable/unsubscribable resource main data

You can display and edit multi requestable/unsubscribable resources' main data.

To display and edit a multi requestable/unsubscribable resource's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **Multi requestable/unsubscribable resources**.
3. On the **Multi requestable/unsubscribable Resources** page, click the multi requestable/unsubscribable resource whose main data you want to display/edit.
4. In the **Edit Multi Requestable/Unsubscribable Resource** pane.

You can edit the following main data.

Table 84: Multi requestable/unsubscribable resource main data

Property	Description
Multi requestable/unsubscribable resource	Enter a full, descriptive name for the multi requestable/unsubscribable resource.
Resource type	Select the resource type of the multi requestable/unsubscribable resource. Use resource types to group multi requestable/unsubscribable resources.
Description	Enter a description for the multi requestable/unsubscribable resource.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning multi requestable/unsubscribable resources to identities. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Product owner	Click Select/Change and then select an application role. The members of this application role can edit the main data of the multi requestable/unsubscribable resource and be used as approvers in approval processes for multi requestable/unsubscribable resource requests.

5. Click **Save**.

Managing resources

You can use the Web Portal to manage resources.

Detailed information about this topic

- [Displaying resources](#) on page 380
- [Displaying and editing resource main data](#) on page 380

Displaying resources

You can display any of the resources and their details.

To display resources

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Resources**.
This opens the **Resources** page and displays all the resources.
3. (Optional) To display details of a resource, click the resource.

Displaying and editing resource main data

You can display and edit resources' main data.

To display and edit a resource's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **Resources**.
3. On the **Resources** page, click the resource whose main data you want to display/edit.
4. In the **Edit Resource** pane.

You can edit the following main data.

Table 85: Resource main data

Property	Description
Resource	Enter a full, descriptive name for the resource.
Resource type	Select a resource type for the resource. Use resource types to group resources.
Description	Enter a description for the resource.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning resources to identities. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Product owner	Click Select/Change and then select an application role. The members of this application role can edit the main data of the resource and be used as approvers in approval processes for resource requests.

5. Click **Save**.

Managing locations

You can use the Web Portal to manage locations.

Detailed information about this topic

- [Displaying locations](#) on page 382
- [Creating locations](#) on page 382
- [Displaying and editing location main data](#) on page 383
- [Copying/splitting locations](#) on page 385
- [Comparing and merging locations](#) on page 386
- [Restoring locations to their previous state](#) on page 387
- [Managing location memberships](#) on page 388
- [Managing location entitlements](#) on page 391
- [Displaying location rule violations](#) on page 393
- [Location history](#) on page 393
- [Restoring deleted locations](#) on page 395

Displaying locations

You can display any of the locations and their details.

To display locations

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Departments**.
This opens the **Locations** page and displays all the locations.
3. (Optional) To display details of a location, click the location.

Creating locations

You can create new locations.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a location

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Departments**.
3. On the **Locations** page, click **+ Create locations**.
4. In the **Create Location** pane, enter the main data of the location in the respective fields.

You can edit the following main data.

Table 86: Location main data

Property	Description
Location	Enter a full, descriptive name for the location.
Short name	Enter a short name for the location.
Name	Enter an additional description for the location.
Parent location	Click Select/Change and select a location to be the parent location for organizing the location hierarchically. If you want the location at the root of a location hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the location.
Deputy manager	Select an identity to act as a deputy to the location's manager.
Additional manager	Click Select/Change and select an application role. Members of the selected application role are responsible for the location.
Attestor	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the location.
Department	Click Select/Change and select the department the location is primarily assigned to.
Cost center	Click Select/Change and select the cost center the location is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the location.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the location.
Description	Enter a description for the location.

5. Click **Create**.

Displaying and editing location main data

You can display and edit locations' main data.

To display and edit a location's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **Locations**.
3. On the **Locations** page, click the locations whose main data you want to display/edit.
4. In the **Edit Location** pane.

You can edit the following main data.

Table 87: Location main data

Property	Description
Location	Enter a full, descriptive name for the location.
Short name	Enter a short name for the location.
Name	Enter an additional description for the location.
Parent location	Click Select/Change and select a location to be the parent location for organizing the location hierarchically. If you want the location at the root of a location hierarchy, leave the field empty.
Manager	Select the manager who is responsible for the location.
Deputy manager	Select an identity to act as a deputy to the location's manager.
Additional manager	Click Select/Change and select an application role. Members of the selected application role are responsible for the location.
Attestor	Click Select/Change and select an application role. Members of the selected application role can approve attestation cases for the location.
Department	Click Select/Change and select the department the location is primarily assigned to.
Cost center	Click Select/Change and select the cost center the location is primarily assigned to.
Role approver	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the location.
Role approver (IT)	Click Select/Change and select an application role. Members of the selected application role can approve requests for members of the location.
Description	Enter a description for the location.

5. Click **Save**.

Copying/splitting locations

You can copy or move memberships and entitlements from locations you are responsible for to new objects (departments, business roles, cost centers, locations).

To copy a location or move memberships and entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location you want to copy or whose memberships and entitlements you want to move.
4. In the **Edit Location** pane, click **⋮ (Actions) > Split**.
5. In the **Split** pane, in the **Type of new object** menu, select which type to give the new object.
6. Depending on the object type you have selected, enter the basic main data of the new object in the corresponding fields.

TIP: After the object has been created, you can add the remaining main data (see [Displaying and editing my department main data](#) on page 171, [Displaying and editing my business roles' main data](#) on page 202, [Displaying and editing my cost center main data](#) on page 236, or [Displaying and editing my locations' main data](#) on page 265).

7. Click **Next**.
8. In the **Select assignments to be copied or moved to the new object** step, perform the following actions:
 - To neither copy nor move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and do not copy or move to new object**. The entitlement/membership is later only available in the source object.
 - To copy or move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Keep and copy new object**. The entitlement/membership is included later in the source object as well as the target object.
 - To move an entitlement or a membership to a new object, in the menu next to the corresponding entitlement/membership, select **Move to new object**. The entitlement/membership is later removed from the source object and only included in the target object.
9. Click **Next**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Next**.

Related topics

- [Managing location memberships](#) on page 388
- [Managing location entitlements](#) on page 391

Comparing and merging locations

You can compare properties of locations with the properties of other business roles, departments, cost centers, or locations that you are also responsible for. Then you can take the properties that you want and merge them together.

To compare and merge a location

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location you want to compare and merge.
4. In the **Edit Location** pane, click **⋮ (Actions) > Compare and merge**.
5. In the **Compare and Merge** pane, in the **Comparison object** field, click **Select**.
6. In the **Edit Property** pane, in the **Selected table** menu, select whether you want to compare and merge the location with a business role, department, cost center, or location.
7. Click the relevant business role, department, cost center, or location.
8. Click **Continue**.

The assigned memberships and entitlements of both objects are listed with the following information in the **View comparison result** step.

Table 88: Overview of the assignments

Column	Description
Assigned object	Shows you the name of the assigned entitlement/membership that occurs in one of the selected objects being compared.

Column	Description
This object	<p>Shows you the assignment type of the entitlement/membership in the source or comparison object. The following assignment types are available.</p> <ul style="list-style-type: none"> • Direct • Inherited • Requested • Dynamic • Not assigned <p>For more detailed information about assigning company resources, see the <i>One Identity Manager Identity Management Base Module Administration Guide</i>.</p>
Comparison object	

9. Click **Continue**.
10. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
11. Click **Merge**.

Related topics

- [Managing location memberships](#) on page 388
- [Managing location entitlements](#) on page 391

Restoring locations to their previous state

You can compare the current status of a location to its status at another time and completely or partially restore the historical state.

To restore a location to a previous state

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location you want to roll back.
4. In the **Edit Location** pane, click **(Actions) > Reset to previous state**.
5. In the **Reset to Previous State** pane, specify a date in the date field. This displays all changes that have taken place since the given date.
6. Select the check box next to the property that you want to restore to its previous state.
7. Click **Next**.

8. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
9. Click **Next**.

Related topics

- [Managing location memberships](#) on page 388
- [Managing location entitlements](#) on page 391

Managing location memberships

As soon as an identity is assigned to a location, the identity becomes a member in the location.

Detailed information about this topic

- [Displaying location memberships](#) on page 388
- [Analyzing assignments to locations](#) on page 388
- [Adding identities to locations](#) on page 389
- [Removing identities from locations](#) on page 391

Displaying location memberships

You can display which identities are assigned to certain locations.

To display memberships

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location whose memberships you want to display.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. (Optional) To display all primary memberships, click **Primary memberships**.
6. (Optional) To view all secondary memberships, click **Secondary memberships**.
7. (Optional) To display all members who were originally assigned through a dynamic role but have been excluded, click **Excluded members**.

Analyzing assignments to locations

You can display how a location assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location whose memberships you want to display.
4. On the **Edit Location** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click the membership to display its assignment analysis.

Adding identities to locations

You can add identities to locations.

The following assignment options are available:

- Assignment by [request](#)
- Automatic assignment through a [dynamic role](#)
- Revoking [exclusion](#) of a member

To assign an identity to a location using a request

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location to which you want to add an identity.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Click **Request memberships**.
7. In the **Request Memberships** pane, next to the identity to which you want to assign the location, select the check box.
8. Click **Request memberships**.
9. Close the **Edit Location** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

Once the request has been granted approval, the identity is assigned to the location.

To add members automatically through a dynamic role

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location for which you want to create a dynamic role.
4. In the **Edit Location** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Automatic memberships**.
6. Click **Create dynamic role**.
7. Use conditions to specify which identities to add over the dynamic role. Perform the following actions to do this:
 - a. Click **Add condition**.
 - b. In the **Property** menu, select the relevant property.
 - c. In the **Operator** menu, select a logical operator.
 - d. In the final field, specify a comparison value.
 - e. (Optional) To add another condition, click **Add another condition** and repeat the steps.
 - f. (Optional) To change the way the conditions are linked, you can toggle between **And** and **Or** by clicking the link.

TIP: To remove a condition, click  (**Delete**).

For more information about customizing filter conditions, see [Custom filter conditions](#) on page 28.

8. Click **Save**.
9. (Optional) In the **Calculation schedule** menu, select the schedule that specifies when memberships are calculated.
10. (Optional) To calculate memberships immediately after a relevant object is changed, select the **Assignments recalculated immediately** check box.
11. Click **Save**.

TIP: A membership that was created through a dynamic role is labeled as **Assigned by dynamic role** in the memberships list.

To re-add an excluded member

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location to which you want to re-add a member.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.
6. Select the check box next to the identity you want to re-add as a member.
7. Click **Remove exclusion**.

Related topics

- [Requesting products](#) on page 71

Removing identities from locations

You can remove identities from locations by deleting the corresponding memberships.

To remove a location from an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location that has a membership you want to delete.
4. In the **Edit Location** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Secondary Memberships**.
6. Select the check box next to the membership you want to delete.
7. Click **Remove**.
8. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
9. Click **Delete memberships**.

TIP: If you only selected direct memberships, confirm the prompt in the **Remove Memberships** dialog with **Yes**.

Managing location entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. By assigning entitlements to locations you avoid having to assign entitlements separately to each identity because all the identities are automatically assigned to the locations.

Detailed information about this topic

- [Displaying location entitlements](#) on page 391
- [Adding entitlements to locations](#) on page 392
- [Deleting entitlements from locations](#) on page 392

Displaying location entitlements

You can display entitlements assigned to locations.

To display entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location whose entitlements you want to display.
4. In the **Edit Location** pane, click the **Entitlements** tab.

Adding entitlements to locations

You can add entitlements to locations. You do this through a request.

To add an entitlement to a location

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location to which you want to add an entitlement.
4. In the **Edit Location** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.
8. Click **Apply**.
9. Close the **Edit Location** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.

After the request has been granted approval, the entitlement is added to the location.

Related topics

- [Requesting products](#) on page 71

Deleting entitlements from locations

You can delete entitlements assigned to locations.

To delete an entitlement from a location

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location whose entitlements you want to delete.

4. In the **Edit Location** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying location rule violations

You can display location rule violations.

To display rule violations

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location whose rule violations you want to display.
4. On the **Edit Location** pane, click the **Rule Violations** tab.

Location history

The Web Portal allows you to display historical data of locations.

To do this, you have the following options:

Table 89: Historical data

View	Description
Events	Shows all events relating to the location in table form (see Displaying location history on page 394).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of locations on page 394).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of locations on page 394).

Displaying location history

To track changes, you can display locations' history.

To display the history

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location whose history you want to display.
4. On the **Edit Location** pane, click the **History** tab.

Displaying the status overview of locations

You can display all the changes effecting locations for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location whose status overview you want to display.
4. In the **Edit Location** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of locations

You can compare the current status of a location that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click the location whose status you want to compare.
4. In the **Edit Location** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Restoring deleted locations

You can restore deleted locations. For example, a location can be deleted if two roles are merged (see [Comparing and merging locations](#) on page 386).

To restore a deleted location

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **Locations**.
3. On the **Locations** page, click **Restore deleted object**.
4. In the **Restore Deleted Object** pane, click the location that you want to restore.
5. Click **Next**.
6. (Optional) In the **Verify actions** step, verify the actions to run and deselect the check box in front of any actions that should not be run.
7. Click **Next**.

Managing system entitlements

You can use the Web Portal to manage system entitlements.

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

Detailed information about this topic

- [Displaying system entitlements](#) on page 396
- [Making system entitlements requestable](#) on page 396
- [Displaying and editing system entitlements main data](#) on page 397
- [Specifying system entitlement owners](#) on page 398
- [Managing service items for system entitlements](#) on page 400
- [Managing system entitlement memberships](#) on page 407
- [Managing system entitlement child groups](#) on page 409
- [System entitlement history](#) on page 410
- [Managing attestation cases of system entitlements](#) on page 412
- [Creating reports about system entitlements](#) on page 413

Displaying system entitlements

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

To display system entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Business roles**.
This opens the **System Entitlements** page and displays all the system entitlements.
3. (Optional) To display only system entitlements that are assigned to a specific target system, perform the following actions:
 - a. Click  (**target system**).
 - b. In the **Narrow the selection further down by: Target system** dialog, select the target system whose system entitlements you want to display.
TIP: To display target systems that are under a target system, click  (**expand**).
4. (Optional) To display details of a system entitlement, click the system entitlement.

Making system entitlements requestable

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

- The system entitlement must be assigned to a service item (see [Managing service items for system entitlements](#) on page 400).
- The system entitlement must be assigned to a shelf in a shop (see [Adding products to shelves](#) on page 55).
- The system entitlement must be marked as requestable (see following step-by-step).

To make a system entitlement requestable

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

TIP: If you do not want the system entitlement to be requested in the Web Portal anymore, click **⋮ (Actions) > Make not requestable**.

Related topics

- [Managing shops](#) on page 46
- [Managing service items for system entitlements](#) on page 400
- [Adding products to shelves](#) on page 55

Displaying and editing system entitlements main data

You can display and edit system entitlements' main data.

To display and edit a system entitlement's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlements whose main data you want to display/edit.
4. In the **Edit System Entitlement** pane.

You can edit the following main data.

Table 90: System entitlement main data

Property	Description
Name	Enter a full, descriptive name for the system entitlement.
Canonical name	Shows the automatically generated canonical name of the system entitlement.
Distinguished name	Shows the automatically generated distinguished name of the system entitlement.
Display name	Enter a name for displaying the system entitlement in the One Identity Manager tools.
Notes domain	Shows the Notes domain name.
Description	Enter a description for the system entitlement.
Category	Select the category for system entitlement inheritance. User accounts can inherit system entitlements selectively. To do this, system entitlements and user accounts are divided into categories.
IT shop	Enable this check box to allow the system entitlement to be requested through the IT Shop. This system entitlement can be requested by your identities through the Web Portal and allocated by defined approval processes. The system entitlement can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only use in IT Shop	Enable the check box to allow the system entitlement to be requested through the IT Shop if required. This system entitlement can be requested by your identities through the Web Portal and allocated by defined approval processes. The system entitlement may not be assigned directly to hierarchical roles.

5. Click **Save**.

Specifying system entitlement owners

You can specify which identities are responsible for system entitlements. To do this, you must assign one or more product owners to the service item assigned to the system entitlement.

To specify owners for a system entitlement

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Business roles**.
3. On the **System Entitlements** page, click the system entitlement whose owners you want to specify.
4. In the **Edit System EntitlementEdit Software** pane, click the tab.
5. On the **Service Item** tab, perform one of the following actions:
 - To specify members of a specific application role as product owners, perform the following actions:
 1. Under **Product owner**, enable the **Select from roles** option.
 2. In the **Product owner** field, click **Select/Change**.
 3. In the **Edit Property** pane, click the appropriate application role.
 - To specify a specific identity as the product owner, perform the following actions:
 1. Under **Product owner**, enable the **Select from identities** option.
 2. In the **Identity** list, select the corresponding identity.
6. Click **Save**.

To specify owners for several system entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, select the check box in front of the system entitlements whose owners you want to specify.
4. Click **Assign product owner**.
5. In the **Assign Product Owner** pane, perform the following actions:
 - To specify members of a specific application role as product owners, perform the following actions:
 1. Under **Product owner**, enable the **Select from roles** option.
 2. In the **Product owner** field, click **Select/Change**.
 3. In the **Edit Property** pane, click the appropriate application role.
 - To specify a specific identity as the product owner, perform the following actions:
 1. Under **Product owner**, enable the **Select from identities** option.
 2. In the **Identity** list, select the corresponding identity.
6. Click **Apply**.

Managing service items for system entitlements

To be able to request system entitlements as products, they must be allocated to service items that are assigned to a shop (see [Managing requestable products in shops](#) on page 54).

Detailed information about this topic

- [Creating service items for system entitlements](#) on page 400
- [Specifying system entitlement owners](#) on page 398
- [Editing system entitlement service items](#) on page 404

Creating service items for system entitlements

You can create service items for system entitlements.

To create a service item for a system entitlement

1. In the menu bar click **Data administration** > **Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement for which you want to create a service item.
4. In the **Edit System Entitlement** pane, click the **Main Data** tab.
5. On the **Main Data** tab, click **Create service item**.
6. Click **Service Item** tab.
7. On the **Service Item** tab, edit the service item's main data.

You can edit the following main data.

Table 91: Service item main data

Property	Description
Service item	Enter a name for the service item.
Description	Enter a description of the service item.
Service category	You can group different service items into service categories. To do this, click /Select/Change and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 56.

Property	Description
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Approval by multi-factor authentication	Select this check box if approvals of requests for this service item require multi-factor authentication.
Max. days valid	Specify how long an identity can keep the product until it is automatically unsubscribed again. An identity keeps their requested products on the shelf until they unsubscribe from them themselves. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. Products that are intended to have a limited shelf life need to be marked with a validity period.
Website	Specify the URL of a web page that contains more information about the product. Use the following format: https://www.example.com or http://www.example.com . This field allows you to link product descriptions in the internet or intranet to the service item.
Sort order	Specify how the service category is sorted.
Request property	Select the request property using the additional request parameters that are defined for a request. If you do not select any request properties, the request properties of the associated service category are used. Requests can be given additional information though product-specific request properties such as the specific details of a product, its size, or color. A request property gathers all additional features together that can be given when requesting a product.
Functional area	Click Select/Change and then select the functional area to which you want to assign the service item. You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by functional area. To do this, service items must be assigned to functional areas. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Attestor	Click Select/Change and then select an application

Property	Description
	role. Members of this application role can approve attestation cases that affect the service item.
Terms of use	Select the terms of use that the product's requester must accept.
Reason type on request	Select which type of reason is required when the service item is requested. <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on approval	Select which type of reason is required when the service item request is approved. <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on denial	Select which type of reason is required when the service item request is denied. <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Picture	Enter a picture for the service item. Users see this picture when they make a request. Perform the following actions as well: <ol style="list-style-type: none"> 1. Click Add/Change. 2. Select an image from your medium.
Hide in service catalog	Set this check box if the service item is meant to be requestable but is not displayed in the service catalog.

Property	Description
Request parameters must be defined per recipient	Select the check box to enter additional request properties separately for each recipient of the associated product, if the product is requested for several recipients in one request procedure.
Retain service item assignment on relocation	Select the check box if you want requests for this service item to be retained when a customer or the product is moved. If an identity requests a product from a shop and changes the shop at a later date, a decision must be made about how to proceed with the existing request. The same applies if a product is moved to another shelf.
Tags	Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.
Not requestable/Requestable	Set the switch to Requestable if you want to request the product via the Web Portal. Set the switch to Not requestable if you do not want to request the product via the Web Portal.
Product owner	Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item. Specify which identities are responsible for the service item. <ul style="list-style-type: none"> • To specify members of a specific application role as product owners, perform the following actions: <ol style="list-style-type: none"> 1. Under Product owner, enable the Select from roles option. 2. In the Product owner field, click Select/Change. 3. In the Edit Property pane, click the appropriate application role. • To specify a specific identity as the product owner, perform the following actions: <ol style="list-style-type: none"> 1. Under Product owner, enable the Select from identities option. 2. In the Identity list, select the corresponding identity.

8. Click **Save**.

Editing system entitlement service items

You can edit the main data of service items.

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

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Business roles**.
3. On the **System Entitlements** page, click the system entitlement whose service item you want to edit.
4. In the **Edit System EntitlementEdit Software** pane, click the tab.
5. On the **Service Item** tab, edit the service item's main data.

You can edit the following main data.

Table 92: Service item main data

Property	Description
Service item	Enter a name for the service item.
Description	Enter a description of the service item.
Service category	You can group different service items into service categories. To do this, click /Select/Change and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 56.
Approval policy	Select the approval policy used to determine the approver when the service item is requested in the Web Portal.
Approval by multi-factor authentication	Select this check box if approvals of requests for this service item require multi-factor authentication.
Max. days valid	Specify how long an identity can keep the product until it is automatically unsubscribed again. An identity keeps their requested products on the shelf until they unsubscribe from them themselves. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. Products that are intended to have a limited shelf life need to be marked with a validity period.
Website	Specify the URL of a web page that contains more information about the product. Use the following format: https://www.example.com or

Property	Description
	<p>http://www.example.com.</p> <p>This field allows you to link product descriptions in the internet or intranet to the service item.</p>
Sort order	Specify how the service category is sorted.
Request property	<p>Select the request property using the additional request parameters that are defined for a request. If you do not select any request properties, the request properties of the associated service category are used.</p> <p>Requests can be given additional information though product-specific request properties such as the specific details of a product, its size, or color. A request property gathers all additional features together that can be given when requesting a product.</p>
Functional area	<p>Click Select/Change and then select the functional area to which you want to assign the service item.</p> <p>You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by functional area. To do this, service items must be assigned to functional areas. For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p>
Attestor	Click Select/Change and then select an application role. Members of this application role can approve attestation cases that affect the service item.
Terms of use	Select the terms of use that the product's requester must accept.
Reason type on request	<p>Select which type of reason is required when the service item is requested.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on approval	<p>Select which type of reason is required when the service item request is approved.</p> <ul style="list-style-type: none"> • Optional: A reason can be provided if required.

Property	Description
	<ul style="list-style-type: none"> Reason required (standard or free): A standard reason must be selected or a reason given with any text. Free text required: A reason must be given with freely selected text.
Reason type on denial	<p>Select which type of reason is required when the service item request is denied.</p> <ul style="list-style-type: none"> Optional: A reason can be provided if required. Reason required (standard or free): A standard reason must be selected or a reason given with any text. Free text required: A reason must be given with freely selected text.
Picture	<p>Enter a picture for the service item. Users see this picture when they make a request.</p> <p>Perform the following actions as well:</p> <ol style="list-style-type: none"> Click Add/Change. Select an image from your medium.
Hide in service catalog	<p>Set this check box if the service item is meant to be requestable but is not displayed in the service catalog.</p>
Request parameters must be defined per recipient	<p>Select the check box to enter additional request properties separately for each recipient of the associated product, if the product is requested for several recipients in one request procedure.</p>
Retain service item assignment on relocation	<p>Select the check box if you want requests for this service item to be retained when a customer or the product is moved.</p> <p>If an identity requests a product from a shop and changes the shop at a later date, a decision must be made about how to proceed with the existing request. The same applies if a product is moved to another shelf.</p>
Tags	<p>Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.</p>
Not requestable/Requestable	<p>Set the switch to Requestable if you want to request the product via the Web Portal.</p> <p>Set the switch to Not requestable if you do not want</p>

Property	Description
	to request the product via the Web Portal.
Product owner	<p>Product owners can edit service item's main data and, be included in approval procedures as approvers for requests of this service item.</p> <p>Specify which identities are responsible for the service item.</p> <ul style="list-style-type: none"> To specify members of a specific application role as product owners, perform the following actions: <ol style="list-style-type: none"> Under Product owner, enable the Select from roles option. In the Product owner field, click Select/Change. In the Edit Property pane, click the appropriate application role. To specify a specific identity as the product owner, perform the following actions: <ol style="list-style-type: none"> Under Product owner, enable the Select from identities option. In the Identity list, select the corresponding identity.

6. Click **Save**.

Related topics

- [Specifying system entitlement owners](#) on page 398

Managing system entitlement memberships

As soon as a system entitlement has been assigned to an identity using a corresponding user account, the identity becomes a member in the system entitlement.

Detailed information about this topic

- [Displaying system entitlement memberships](#) on page 408
- [Analyzing assignments to system entitlements](#) on page 408
- [Assigning identity system entitlements](#) on page 408
- [Removing system entitlements from identities](#) on page 409

Displaying system entitlement memberships

You can display which identities are assigned to certain system entitlements.

To display memberships

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose memberships you want to display.
4. In the **Edit System Entitlement** pane, click the **Memberships** tab.
5. (Optional) To display all memberships exist directly in the selected system entitlement, click **Direct memberships**.
6. (Optional) To display all memberships created by inheritance from child system entitlements, click **Inherited memberships**.

Analyzing assignments to system entitlements

You can display how a system entitlement assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose memberships you want to display.
4. On the **Edit System Entitlement** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Direct memberships** or **Inherited memberships**.
6. Click the membership to display its assignment analysis.

Assigning identity system entitlements

You can assign system entitlements to identities. You do this through requests.

To assign an identity to a system entitlement using a request

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement to which you want to assign an identity.

4. In the **Edit System Entitlement** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Request memberships**.
6. In the **Request Memberships** pane, next to the identity to which you want to assign the system entitlement, select the check box.
7. Click **Apply**.
8. Close the **Edit System Entitlement** pane.
9. In the menu bar, click **Requests > Shopping cart**.
10. On the **Shopping Cart** page, click **Submit**.

Once the request has been granted approval, the identity is assigned to the system entitlement.

Related topics

- [Requesting products](#) on page 71

Removing system entitlements from identities

You can remove system entitlements from identities by deleting or unsubscribing the relevant memberships.

To remove a system entitlement from an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement with a membership you want to delete.
4. In the **Edit System Entitlement** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Direct Memberships**.
6. Select the check box next to the membership you want to delete.
7. Perform one of the following actions:
 - If it is a direct assignment, click **Remove**.
 - If it is an assignment request, click **Unsubscribe**.
8. In the **Remove Memberships** or **Unsubscribe Memberships** dialog, confirm the prompt with **OK**.

NOTE: You can only unsubscribe memberships that you have requested yourself.

Managing system entitlement child groups

You can order more groups under certain group types or order these under other groups:

- Active Directory groups
- LDAP groups
- Notes groups
- Custom target systems groups

Detailed information about this topic

- [Displaying system entitlements' child groups](#) on page 410

Displaying system entitlements' child groups

You can display child groups of system entitlements.

To display the child groups of a system entitlement

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose child groups you want to display.
4. In the **Edit System Entitlement** pane, click the **Child System Entitlements** tab.

System entitlement history

The Web Portal allows you to display historical data of system entitlements.

To do this, you have the following options:

Table 93: Historical data

View	Description
Events	Shows all events relating to the system entitlement in table form (see Displaying system entitlement history on page 411).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of system entitlements on page 411).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of system entitlements on page 411).

Displaying system entitlement history

To track changes, you can display system entitlements' history.

To display the history

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose history you want to display.
4. On the **Edit System Entitlement** pane, click the **History** tab.

Displaying the status overview of system entitlements

You can display all the changes effecting system entitlements for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose status overview you want to display.
4. In the **Edit System Entitlement** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of system entitlements

You can compare the current status of a system entitlement that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose status you want to compare.
4. In the **Edit System Entitlement** pane, click the **History** tab.

5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Managing attestation cases of system entitlements

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

Detailed information about this topic

- [Displaying attestation cases of system entitlements](#) on page 412
- [Approving and denying attestation cases of system entitlements](#) on page 413

Displaying attestation cases of system entitlements

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

To display attestation cases of a system entitlement

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose attestation cases you want to display.
4. In the **Edit System Entitlement** pane, click the **Attestation** tab.
This displays all the system entitlement's attestation cases.
5. (Optional) To display more details of an attestation case, click the corresponding attestation case.

Related topics

- [Attestation](#) on page 113
- [Displaying pending attestation cases](#) on page 137

Approving and denying attestation cases of system entitlements

You can make an approval decision about certain system entitlement attestation cases (approve or deny).

To approve an attestation case

1. In the menu bar click **Data administration > Data Explorer**.
 2. In the Data Explorer navigation, click **System entitlements**.
 3. On the **System Entitlements** page, click the system entitlement whose attestation cases are pending your approval.
 4. In the **Edit System Entitlement** pane, click the **Attestation** tab.
 5. On the **Attestation** tab, click **▼ (Filter)**.
 6. In the filter context menu, under **State**, select the **Pending** option.
 7. Perform one of the following actions:
 - To approve an attestation case, select the check box next to the attestation case in the list and click **Approve** below the list.
 - To deny an attestation case, select the check box next to the attestation case in the list and click **Deny** below the list.
 8. (Optional) In the **Approve Attestation Case** or the **Deny Attestation Case** pane, perform the following actions:
 - a. In the **Reason for your decision** field, select a standard reason for your approval decision.
 - b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.
- TIP:** By giving reasons, your approvals are more transparent and support the audit trail.
9. Click **Save**.

Related topics

- [Attestation](#) on page 113
- [Approving or denying attestation cases](#) on page 138

Creating reports about system entitlements

You can create reports on system entitlement data.

To create a report on a system entitlement

1. In the menu bar click **Data administration > Data Explorer**.
2. In the data explorer, click **system entitlements**.
3. On the **System Entitlements** page, click the system entitlement that you want to create a report on.
4. In the **Edit System Entitlement**, click **Download report**.

Managing system roles

You can use the Web Portal to manage system roles.

Detailed information about this topic

- [Displaying system roles](#) on page 414
- [Creating system roles](#) on page 414
- [Displaying and editing system role main data](#) on page 416
- [Managing system role memberships](#) on page 417
- [Managing system role entitlements](#) on page 420
- [Displaying system role rule violations](#) on page 421
- [System role history](#) on page 422

Displaying system roles

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

To display system roles

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Application roles**.
This opens the **System Roles** page and displays all the System roles.
3. (Optional) To display details of a system role, click the system role.

Creating system roles

You can create new system roles.

Other properties (such as, memberships, entitlements, and so on) can be defined later during editing.

To create a system role

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Application roles**.
3. On the **System Roles** page, click **+ Create system role**.
4. In the **Create System Role** pane, enter the main data of the system role in the respective fields.

You can edit the following main data.

Table 94: System role main data

Property	Description
System role	Enter a full, descriptive name for the system role.
Display name	Enter a name for displaying the system role in the One Identity Manager tools.
Internal product name	Enter a company internal name for the system role.
System role type	Select the role type of the system role. The system role type specifies which type of company resources make up the system role.
Service item	Shows you the associated service item.
System role manager	Click Change and select the identity responsible for the system role. This identity can edit the system role's main data and be used as an attestor for system role properties. If the system role can be requested in the IT Shop, the manager will automatically be a member of the application role for product owners assigned the service item.
Comment	Enter a comment for the system role.
IT shop	Select the check box if the system role can also be requested through the IT Shop. This system role can be requested by identities through the Web Portal and allocated by defined approval processes. The system role can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only use in IT Shop	Select the check box if the system role can only be requested through the IT Shop. This system role can be requested by identities through the Web Portal and allocated by defined approval processes. The system role may not be assigned directly to hierarchical roles.

5. Click **Create**.

Displaying and editing system role main data

You can display and edit the business roles' main data.

To display and edit a system role's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **System roles**.
3. On the **System Roles** page, click the system role whose main data you want to display.
4. In the **Edit System Role** pane.

You can edit the following main data.

Table 95: System role main data

Property	Description
System role	Enter a full, descriptive name for the system role.
Display name	Enter a name for displaying the system role in the One Identity Manager tools.
Internal product name	Enter a company internal name for the system role.
System role type	Select the role type of the system role. The system role type specifies which type of company resources make up the system role.
Service item	Shows you the associated service item.
System role manager	Click Change and select the identity responsible for the system role. This identity can edit the system role's main data and be used as an attestor for system role properties. If the system role can be requested in the IT Shop, the manager will automatically be a member of the application role for product owners assigned the service item.
Comment	Enter a comment for the system role.
IT shop	Select the check box if the system role can also be requested through the IT Shop. This system role can be requested by identities through the Web Portal and allocated by defined approval processes. The system role can still be assigned directly to identities and hierarchical roles. For more information about IT Shop, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only use in IT Shop	Select the check box if the system role can only be requested through the IT Shop. This system role can be requested by identities through the Web Portal and allocated by defined approval processes. The system role may not be assigned directly to hierarchical roles.

5. Click **Save**.

Managing system role memberships

As soon as a system role is assigned to an identity, the identity becomes a member in the system role.

Detailed information about this topic

- [Displaying system role memberships](#) on page 418
- [Analyzing assignments to system roles](#) on page 418
- [Assigning identities to system roles](#) on page 418
- [Removing identities from my system roles](#) on page 419

Displaying system role memberships

You can display which identities are assigned to certain system roles.

To display memberships

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role whose memberships you want to display.
4. In the **Edit System Role** pane, click the **Memberships** tab.

Analyzing assignments to system roles

You can display how a system role assignment came about by displaying an assignment analysis for the corresponding membership.

To display the assignment analysis for a membership

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role whose memberships you want to display.
4. On the **Edit System Role** pane, click the **Memberships** tab.
5. Click the membership to display its assignment analysis.

Assigning identities to system roles

You can assign system roles to identities. You do this through requests.

To assign an identity to a system role using a request

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

3. On the **System Roles** page, click the system role to which you want to assign an identity.
4. In the **Edit System Role** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Request memberships**.
6. In the **Request Memberships** pane, next to the identity to which you want to assign the system role, select the check box.
7. Click **Request memberships**.
8. Close the **Edit System Role** pane.
9. In the menu bar, click **Requests > Shopping cart**.
10. On the **Shopping Cart** page, click **Submit**.
Once the request has been granted approval, the identity is assigned to the system role.

Related topics

- [Requesting products](#) on page 71

Removing identities from my system roles

You can remove identities from system roles by deleting the corresponding memberships.

To remove a system role from an identity

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role that has a membership you want to delete.
4. In the **Edit System Role** pane, click the **Memberships** tab.
5. Select the check box next to the membership you want to delete.
6. Click **Remove**.
7. (Optional) In the **Remove Memberships** pane, perform the following:
 - For assignment requests: In the **Reason for unsubscribing the membership** field, enter why you want to remove the membership.
 - For memberships assigned through dynamic roles: In the **Reason for excluding the members** field, enter why you want to delete the memberships.
8. Click **Delete memberships**.

TIP: If you only selected direct memberships, confirm the prompt in the **Remove Memberships** dialog with **Yes**.

Managing system role entitlements

Identities can be assigned entitlements to different objects, such as, groups, accounts, roles, or applications. Assigning identities to system roles avoids you having to assign entitlements separately to each identity. All a system role's entitlements are automatically assigned to all the identities assigned to the system role.

Detailed information about this topic

- [Displaying system role entitlements](#) on page 420
- [Adding entitlements to system roles](#) on page 420
- [Deleting system role entitlements](#) on page 421

Displaying system role entitlements

You can display entitlements assigned to system roles.

To display entitlements

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role whose entitlements you want to display.
4. In the **Edit System Role** pane, click the **Entitlements** tab.

Adding entitlements to system roles

You can add entitlements to system roles. You do this through a request.

To add an entitlement to a system role

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role to which you want to add an entitlement.
4. In the **Edit System Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, click **Request entitlements**.
6. In the **Request Entitlements** dialog, in the **Select the type of entitlement to add** menu, select which type of entitlement you want to add.
7. Next to the entitlement you want to add, select the check box.

8. Click **Apply**.
9. Close the **Edit System Role** pane.
10. In the menu bar, click **Requests > Shopping cart**.
11. On the **Shopping Cart** page, click **Submit**.
After the request has been granted approval, the entitlement is added to the system role.

Related topics

- [Requesting products](#) on page 71

Deleting system role entitlements

You can delete entitlements assigned to system roles.

To delete an entitlement from a system role

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role whose entitlements you want to delete.
4. In the **Edit System Role** pane, click the **Entitlements** tab.
5. On the **Entitlements** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. Confirm the prompt with **Yes** in the dialog.

Displaying system role rule violations

You can display system role rule violations.

To display rule violations

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role whose rule violations you want to display.
4. On the **Edit System Role** pane, click the **Rule Violations** tab.

System role history

The Web Portal allows you to display historical data of system roles.

To do this, you have the following options:

Table 96: Historical data

View	Description
Events	Shows all events relating to the system role in table form (see Displaying system role history on page 422).
Status overview	This shows you an overview of all assignments. It also shows you how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between (see Displaying the status overview of system roles on page 422).
Status comparison	You can select a date and display all the changes made from then until now. This also shows you what the value of the property was at the selected point in time and what the value is now (see Comparing statuses of system roles on page 423).

Displaying system role history

To track changes, you can display system roles' history.

To display the history

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role whose history you want to display.
4. On the **Edit System Role** pane, click the **History** tab.

Displaying the status overview of system roles

You can display all the changes effecting system roles for which you are responsible. You can also display how long each change was valid for. Use the status overview to track when changes were made and by whom. This way, you not only see the initial and current status but you also see all the steps in between.

To display the status overview

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role whose status overview you want to display.
4. In the **Edit System Role** pane, click the **History** tab.
5. On the **History** tab, select **Status overview** in the menu.

Comparing statuses of system roles

You can compare the current status of a system role that you are responsible for to its status at another time.

To compare statuses

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, click the system role whose status you want to compare.
4. In the **Edit System Role** pane, click the **History** tab.
5. On the **History** tab, select **Status comparison** in the menu.
6. In the date field, select the date and time from which you want to start the comparison.

Managing assignment resources

You can use the Web Portal to manage assignment resources.

Detailed information about this topic

- [Displaying assignment resources](#) on page 423
- [Displaying and editing assignment resource main data](#) on page 424

Displaying assignment resources

You can display any of the assignment resources and their details.

To display assignment resources

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation, click **Assignment resources**.
This opens the **Assignment Resources** page and displays all the resources.
3. (Optional) To display details of an assignment resource, click the assignment resource.

Displaying and editing assignment resource main data

You can display and edit assignment resources' main data.

To display and edit an assignment resource's main data

1. In the menu bar click **Data administration > Data Explorer**.
2. In the navigation of the Data Explorer, click **Assignment resources**.
3. On the **Assignment Resources** page, click the assignment resource whose main data you want to display/edit.
4. In the **Edit Assignment Resource** pane.

You can edit the following main data.

Table 97: Assignment resource main data

Property	Description
Assignment resource	Enter a full, descriptive name for the assignment resource.
Resource type	Select the resource type of the assignment resource. Use resource types to group assignment resources.
Description	Enter a full, descriptive name for the assignments resource.
Risk index	Use the ruler to specify a risk index range. This value is used to assess the risk of assigning assignment resources to identities. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .

5. Click **Save**.

Opening other web applications

You can access other web applications through related links.

To open other web applications

1. In the menu bar, click **Links > Other web applications**.
2. In the **Other Web Applications** pane, click the web application you want to open.

Managing tickets

Tickets are used to manage support, help, or solve problems, queries, or concerns of users.

Detailed information about this topic

- [Display tickets](#) on page 426
- [Displaying ticket history](#) on page 426
- [Creating tickets](#) on page 427
- [Editing tickets](#) on page 427
- [Managing ticket attachments](#) on page 428

Display tickets

To obtain an overview, you can display all the tickets that you created and are assigned to you.

To display all tickets

1. In the menu bar, click **Help desk > Tickets**.
This opens the **Tickets** page.
2. (optional) To view details of a ticket, click the corresponding ticket.

Detailed information about this topic

- [Displaying ticket history](#) on page 426

Displaying ticket history

To obtain an overview of all the changes made to a ticket, you can display the ticket's history.

To display the history of ticket

1. In the menu bar, click **Help desk > Tickets**.
2. On the **Tickets** page, click the ticket whose history you want to display.
3. In the **Edit Ticket** pane, click the **History** tab.
4. (Optional) To display details of a change, click the appropriate change.

Creating tickets

If you have issues with or questions about products, a software or services, you can create tickets to get support. These tickets contain information about the issues and help desk staff can respond to them to identify the issues and provide solutions.

To create a ticket

1. In the menu bar, click **Help desk > Tickets**.
2. On the **Tickets** page, click **+ Create ticket**.
3. In the **Create Ticket** pane, in the **Description** field, enter a detailed description of the problem.
4. In the **Severity** menu, select a level for the problem.
5. In the **Product** menu, select the product that the problem relates to.
6. Click **Create**.

TIP: To add more information to the ticket, edit the ticket (see [Editing tickets](#) on page 427).

Editing tickets

To provide more information about tickets, you can edit them.

To edit a ticket

1. In the menu bar, click **Help desk > Tickets**.
2. On the **Tickets** page, click the ticket that you want to edit.
3. In the **Edit Ticket** pane, change the main data of the ticket.

You can edit the following main data.

Table 98: Tickets main data

Property	Description
Description	Enter a description of the issue.
Measures	Describe the measures to introduce to solve the issue.
Severity	Select a severity level for the issue: <ul style="list-style-type: none">• Level 1: Critical business impact• Level 2: Significant business impact• Level 3: Minimal business impact• Level 2: Nominal business impact
Product	Select the affected product.
External escalation level	Select the escalation level.
Ticket type	Click Select/Change and then select the ticket type.
Additional staff	Select an identity that can also provide information about the issue.
Ticket status	Select the ticket status.

4. Click **Save**.

Managing ticket attachments

Attachments allow users to attach screenshots, log files, error messages, or other relevant documents directly to tickets. This additional information gives the help desk staff greater insight into the problem and makes it easier to diagnose.

Detailed information about this topic

- [Displaying ticket attachments](#) on page 429
- [Attaching files to tickets](#) on page 429
- [Downloading ticket attachments](#) on page 429
- [Creating folders for ticket attachments](#) on page 430
- [Deleting ticket attachments and folders](#) on page 430

Displaying ticket attachments

To obtain an overview, you can display all the files that are attached to tickets.

To display ticket attachments

1. In the menu bar, click **Help desk > Tickets**.
2. On the **Tickets** page, click the ticket whose attachments you want to display.
3. In the **Edit Ticket** pane, click **Attachments**.
4. (Optional) To display attachments in folders, next to the relevant folder, click **> (expand)**.

Attaching files to tickets

To make files (like screenshots, log files, error messages) available to others, you can attach them to tickets.

NOTE: Attach only relevant information and protect or anonymize sensitive or private data accordingly to respect privacy.

To attach a file to a ticket

1. In the menu bar, click **Help desk > Tickets**.
2. On the **Tickets** page, click the ticket to which you want to attach a file.
3. In the **Edit Ticket** pane, click **Attachments**.
4. (Optional) To attach the file in a folder, click the relevant folder.
5. Click **+ Attach file**.
6. In the dialog, select the file you want to attach and confirm.

Downloading ticket attachments

You can download file attached to tickets in order to save them locally.

To download a ticket attachment

1. In the menu bar, click **Help desk > Tickets**.
2. On the **Tickets** page, click the ticket whose attachments you want to download.
3. In the **Edit Ticket** pane, click **Attachments**.
4. (Optional) To display attachments in folders, next to the relevant folder, click **> (expand)**.

5. Click the file to download.
6. Click  **Download selected file.**

Creating folders for ticket attachments

To organize and structure ticket attachments, you can create folders.

To create a folder

1. In the menu bar, click **Help desk > Tickets**.
2. On the **Tickets** page, click the ticket whose attachments or folders you want to create.
3. In the **Edit Ticket** pane, click **Attachments**.
4. (Optional) To create the new folder as a subfolder of an existing folder, click the relevant folder.
5. Click  **Create folder**.
6. In the **Create Folder**, in the **Folder name** field, enter a name for the new folder.
7. Click **Create**.

Deleting ticket attachments and folders

If there are ticket attachments or folders that you do not need anymore, you can delete them.

NOTE: To delete a folder, delete all the files and subfolders in it first. You cannot delete folders that still contain files or other folders.

To delete a ticket attachment or folder

1. In the menu bar, click **Help desk > Tickets**.
2. On the **Tickets** page, click the ticket whose attachments or folders you want to delete.
3. In the **Edit Ticket** pane, click **Attachments**.
4. (Optional) To display attachments in folders or subfolders, next to the relevant folder, click  (**expand**).
5. Click the ticket attachment or folder you want to delete.
6. Click  **Delete selected item**.
7. In the **Delete File /Delete Folder** dialog, confirm the prompt with **Yes**.

Appendix: Attestation conditions and approval policies from attestation procedures

When attestation policies are created or edited (see [Setting up attestation policies](#) on page 116 or [Editing attestation policies](#) on page 118), you specify attestation conditions and approval policies:

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

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

Attesting primary departments

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

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

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

Attesting primary business roles

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

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

Attesting primary cost centers

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

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

Attesting primary locations

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

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

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

Attesting secondary departments

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

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

Attesting secondary cost centers

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

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

Attesting secondary locations

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

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

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

Attesting PAM asset groups

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

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

Attesting PAM asset accounts

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

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

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

Attesting PAM assets

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

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

Attesting PAM user groups

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

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

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

Attesting PAM user accounts

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

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

Attesting PAM account groups

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

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

Attesting PAM directory accounts

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

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

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

Attesting PAM accesses

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

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

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

Attesting departments

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

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

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

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

Approval policies	Description
Attestation by selected approvers	In the Attestors field, click Select/Change and select the identities that can make approval decisions about attestation cases.
Attestation of departments by manager	Department managers can make approval decisions through attestation cases.

Application role attestation

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

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

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

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

Approval policies	Description
Attestation by selected approvers	In the Attestors field, click Select/Change and select the identities that can make approval decisions about attestation cases.

Business role attestation

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

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

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

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

Approval policies	Description
Attestation by selected approvers	In the Attestors field, click Select/Change and select the identities that can make approval decisions about attestation cases.
Attestation of business roles by manager	Business role managers can make approval decisions through attestation cases.
Certification of business roles	Business role managers can make approval decisions through attestation cases.

Attesting system roles

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

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

Condition	Description
All cost centers	Attests all cost centers.
Specific cost centers	Select the cost centers to attest. Use  and  to switch between hierarchical and list view. Multi-

Condition	Description
	select is possible.
Cost centers with defined risk index	Use the Lower limit and Upper limit fields to define a risk index range. Attests cost centers with a risk index in the chosen range.
Cost centers with matching name	Enter part of a name of cost centers with access to attest. All cost centers that have this pattern in their name are included. Example: Per finds "Person", "Personal", "Perfection" and so on.

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

Approval policies	Description
Attestation by selected approvers	In the Attestors field, click Select/Change and select the identities that can make approval decisions about attestation cases.
Attestation of cost centers by manager	Cost center managers can make approval decisions through attestation cases.

Attesting locations

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

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

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

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

Approval policies	Description
Attestation by selected approvers	In the Attestors field, click Select/Change and select the identities that can make approval decisions about attestation cases.
Attestation of locations by manager	Location managers can make approval decisions through attestation cases.

Attesting system roles

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

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

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

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

Approval policies	Description
Attestation by selected approvers	In the Attestors field, click Select/Change and select the identities that can make approval decisions about attestation cases.
Attestation of system roles by manager	System role managers can make approval decisions through attestation cases.

Attesting memberships in system entitlements

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

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

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

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

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

Approval policies	Description
Attestation by selected approvers	In the Attestors field, click Select/Change and select the identities that can make approval decisions about attest-

Approval policies	Description
	ation cases.
Attestation by selected approvers with automatic removal of assignments	In the Attestors field, click Select/Change and select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.
Attestation by entitlement owner with automatic removal of assignments	Product owners of system entitlements can be approved through attestation cases. Memberships are deleted if attestation is denied and the configuration fits.
Attestation by identity manager and product owner (with peer group analysis)	The following identities can be approved through attestation cases: <ul style="list-style-type: none"> • Identity managers who are assigned the system entitlements • Product owners of system entitlements after a peer group analysis (see Attestation by peer group analysis on page 129)
Attestation of group memberships by product owner with automatic removal of memberships	Product owners of system entitlements can be approved through attestation cases. Memberships are deleted if attestation is denied and the configuration fits.

Attesting memberships in application roles

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

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

Condition	Description
All roles	Attests memberships in all applications roles.
Application roles with matching name	Enter part of a name of application roles with primary memberships to attest. All application roles that have this pattern in their name are included. Example: Per finds "Person", "Personal", "Perfection" and so on.
Attesting by attestation status	Select an attestation status Attests memberships in application roles that match this attestation status. You can select the follow status:

Condition	Description
	<ul style="list-style-type: none"> • Denied memberships: Attests memberships that have been denied. • All Memberships: Attests all memberships. • New memberships: Attests memberships that have never been attested.
Specific identities	Select the identities. Attests identity memberships in application roles.
Specific identities with subidentities.	Select the identities. Attests identity memberships in application roles. In addition, this identity's subidentities memberships in application roles are attested.
Specific roles	Select the application roles. Attests memberships in these application roles. Use  and  to switch between hierarchical and list view. Multi-select is possible.
New or not attested for x days	Specify a number of days. Attests memberships in application roles that have not been attested for the defined number of days.
Roles by assignment type	Select how memberships in application roles must be assigned to enable attestation: <ul style="list-style-type: none"> • Directly assigned: Attests memberships that were assigned directly. • By request: Attests memberships that were requested. • By delegation: Attests memberships that were delegated.

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

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

Attestation of memberships in business roles

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

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

Condition	Description
All roles	Attests memberships in all business roles.
Business roles with matching name	Enter part of a name of business roles with memberships to attest. All business roles that have this pattern in their name are included. Example: Per finds "Person", "Personal", "Perfection" and so on.
Attesting by attestation status	Select an attestation status Attests memberships in business roles that match this attestation status. You can select the follow status: <ul style="list-style-type: none">• Denied memberships: Attests memberships that have been denied.• All Memberships: Attests all memberships.• New memberships: Attests memberships that have never been attested.
Specific identities	Select the identities. Attests identity memberships in business roles.
Specific identities with subidentities.	Select the identities. Attests identity memberships in business roles. In addition, this identity's subidentities memberships in business roles are attested.
Specific roles	Select the business roles. Attests memberships in these business roles. Use  and  to switch between hierarchical and list view. Multi-select is possible.
New or not attested for x days	Specify a number of days. Attests memberships in business roles that have not been attested for the defined number of days.
Roles with specific owners	Select the identities. Attests memberships in business roles of identities that are owners of these business roles.
Roles with specific role classes	Select the role classes. Attests membership in business roles of this role class.
Roles with	Use the Lower limit and Upper limit fields to define a risk index

Condition	Description
defined risk index	range. Attests memberships in business roles with a risk index in the chosen range.
Roles with any owner	Attests all memberships in business roles that have an owner.
Roles with owners in departments	Select the departments. Attests all business roles that have an owner in the selected department.
Roles by assignment type	Select how memberships in business roles must be assigned to enable attestation: <ul style="list-style-type: none"> • Directly assigned: Attests memberships that were assigned directly. • By request: Attests memberships that were requested. • By delegation: Attests memberships that were delegated. • By dynamic role: Attests memberships that were attested through dynamic roles.

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

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

Attesting assignment of memberships in system roles

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

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

Condition	Description
All roles	Attests memberships in all system roles.

Condition	Description
System roles with matching name	Enter part of a name of system roles with memberships to attest. All system roles that have this pattern in their name are included. Example: Per finds "Person", "Personal", "Perfection" and so on.
Attesting by attestation status	Select an attestation status Attests memberships in system roles that match this attestation status. You can select the follow status: <ul style="list-style-type: none"> • Denied memberships: Attests memberships that have been denied. • All Memberships: Attests all memberships. • New memberships: Attests memberships that have never been attested.
Specific roles	Select the system roles. Attests memberships in these system roles. Use  and  to switch between hierarchical and list view. Multi-select is possible.
New or not attested for x days	Specify a number of days. Attests memberships in system roles that have not been attested for the defined number of days.
Roles with specific owners	Select the identities. Attests memberships in system roles of identities that are owners of these system roles.
Roles with defined risk index	Use the Lower limit and Upper limit fields to define a risk index range. Attests memberships in system roles with a risk index in the chosen range.
Roles with any owner	Attests all memberships in system roles that have an owner.
Roles with owners in departments	Select the departments. Attests all system roles that have an owner in the selected department.
System roles by applications	Select the applications (Application Governance). Attests memberships in system roles assigned to these applications.
Roles by assignment type	Select how memberships in system roles must be assigned to enable attestation: <ul style="list-style-type: none"> • Directly assigned: Attests memberships that were assigned directly. • By request: Attests memberships that were requested. • Inherited: Attests inherited memberships.

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

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

Attesting device owners

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

Condition	Description
All devices	Attests owners of all the devices.

Attesting system entitlement owners

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

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

Attesting system entitlement owners (initial)

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

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

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

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

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

Attesting user accounts

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

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

Condition	Description
All user accounts	Attests all user accounts.
All privileged user accounts	Attests all privileged user accounts.
User accounts in the target system	Select the target systems. Attests user accounts assigned to these target systems.
User accounts of specific identities	Select the identities. Attests user accounts assigned to these identities.
Specific user accounts	Select the user accounts to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.
User accounts with defined risk index	Specify a risk index range. Attests user accounts with a risk index in the chosen range.
User accounts with matching name	Enter part of a name of user accounts with access to attest. All user accounts that have this pattern in their name are included. Example: Per finds "Person", "Personal", "Perfection" and so on.
User accounts with identities in department	Select the departments. Attests user accounts with identities assigned to these departments.

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

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

Approval policies	Description
Attestation by selected approvers	In the Attestors field, click Select/Change and select the identities that can make approval decisions about attestation cases.
Attestation by target system manager	Target system managers can be approved through attestation cases.

Attesting system entitlements

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

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

Condition	Description
All system	Attests all system entitlements.

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

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

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

Attesting assignment of system entitlement to departments

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

Condition	Description
All departments	Attests assignments of system entitlements to all departments.
All system	Attests assignments of all system entitlements to departments.

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

Attesting assignment of system entitlement to business roles

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

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

Condition	Description
System entitlements with defined risk index	Use the Lower limit and Upper limit fields to define a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to business roles.
System entitlements with matching name	Enter part of a name of system entitlement with assignments to business roles to attest. All system entitlements that have this pattern in their name are included. Example: Per finds "Person", "Personal", "Perfection" and so on.

Attestation of system entitlement assignments to cost centers

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

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

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

Attestation of system entitlement assignments to locations

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

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

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

Attesting assignment of system role assignment to departments

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

Condition	Description
All departments	Assignments of system roles to all departments
All system roles	Attests assignments of all system roles to departments.
Attesting by attestation	Select an attestation status Attests assignments of system roles, matching this attestation status, to departments.

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

Attesting assignment of system roles to business roles

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

Condition	Description
All business	Attests assignments of system roles to all business roles.

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

Cost center system role assignment attestation

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

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

Attesting assignment of system entitlements to locations

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

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

Attesting assignments to system roles

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

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

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

Contacting us

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

Technical support resources

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

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

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

A

- account
 - new 21
- add product to cart 72
- address book
 - display 30
- application roles 184
- approval decision
 - display 110
- approval history
 - display 110
- approve
 - pending request 93
- attestation
 - by peer group 129
 - carry out 113
 - managing attestation policies 114
 - sample 130
 - viewing completed attestations 148
- attestation sample 130

B

- business roles
 - manage 199

C

- change
 - language 34
- configure
 - request function 46

- contact data
 - rework 33
- create
 - service category 57
 - user account 21
- cross-functional product 129

D

- data
 - manage 308
- date format 34
- deactivate
 - email notification 34
- decision
 - escalate 102
- delete
 - service category 61
 - shopping cart 78
- deny
 - pending request 93
- display
 - approval decision 110
 - approval history 110
 - pending request 91
 - requestable product 54
 - service category 56
 - shopping cart 74

E

edit

- service category 59

- shelf details 51

email notification

- deactivate 34

- enable 34

enable

- email notification 34

F

first login 21

G

give reason 76

grant approval

- pending request 93

H

header 39

hold status

- revert 104, 147

I

identity

- add 214

- edit 214

- manage 342

interest group 81

L

language

- change 34

log in 21-22

- Password Reset Portal 22

log out 21, 24

login 22

M

manage

- data 308

- identity 342

- requestable product access 53

- service category 56

- shopping cart 73

- subscription 35

- system entitlements 395

- user accounts 324

menu bar 39

my responsibilities

- manage 168

N

navigate 24

new

- account 21

- user account 21

number format 34

O

organization structure

- manage 169

other identities' products 81

P

PAG 82

PAM 82

password 30, 32

change 32

password question 30

change 30

create 30

delete 30

edit 30

manage 30

specify 30

unlock 30

Password Reset Portal

log in 22

peer group 80-81

peer group analysis

for attestation 129

pending question

answer 111, 149

display 111

pending request

approve 93

deny 93

display 91

grant approval 93

privileged access 82

product

add to shelf 55

cross-functional 129

remove from shelf 55

product bundles

create 65, 67

display 66

edit 65

Q

query

delete 104, 146

send 103

R

reference user 80

request 72-73, 78

privileged access 82

submit 78

request for multiple identities 77

request function

configure 46

set up 46

request history

display 105

request product 72-73, 78

from other identities 80

peer group 81

requestable product

display 54

requestable product access

manage 53

requests

act 71

about a reference user 80

for other recipient 79

from product bundle 82

other identities' products 80

edit pending request 91

extend 107

- failed 77
- invalid 77
- manage 45
- request group 84
- revoke 108
- responsibility
 - application roles 184
- risk assessment
 - modifying risk calculators 163
- rule and policy violation
 - edit pending violations 161
 - view reports about rule and policy violation 152

S

- sample data 130
- save for later 88
- saved for later 88-91
- serve 24
- service category
 - create 57
 - delete 61
 - display 56
 - edit 59
 - manage 56
- set validity period 75
- setup
 - request function 46
- shelf
 - add product 55
 - clean up products 55
- shelf details
 - edit 51
- shopping cart
 - clean up products 74

- delete 74, 78
- display 74
- empty 74
- fill 72
- give reason 76
- manage 73
- move product to another shelf 88
- request for multiple identities 77
- save for later 88
- saved for later 88-91
- set validity period 75
- specify priority 76
- submit 74
- specify priority 76
- start page 38
- structure 38
- submit
 - shopping cart 74
- subscription
 - manage 35
- system entitlements
 - make requestable 396
 - manage 277, 395
 - prepare for request 396
- system roles
 - manage 199

U

- user account
 - create 21
 - new 21
- user accounts
 - manage 324
- user interface 38

V

value format 34