One Identity Manager On Demand

Web Portal User Guide
Copyright 2022 One Identity LLC.
ALL RIGHTS RESERVED.

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

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

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

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

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

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

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

Legend

⚠️ WARNING: A WARNING icon 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 On Demand Web Portal User Guide
Updated - 27 April 2022, 16:11
### Contents

**General tips and getting started**  ......................................................... 13
- Logging in and out ................................................................. 14
  - Logging in ........................................................................... 14
  - Logging in to the Password Reset Portal ............................. 15
  - Logging off ................................................................. 16
- Navigation and use ............................................................... 16
  - Simple navigation ......................................................... 17
  - Search ............................................................................. 18
    - Context searching ....................................................... 19
  - Help ............................................................................... 19
    - Using the help ........................................................... 19
    - Filtering ...................................................................... 20
- Displaying the address book ................................................ 20
- Managing password questions ............................................ 20
  - Creating password questions ........................................... 21
  - Editing password questions .............................................. 21
  - Deleting password questions ........................................... 22
- Changing passwords ............................................................ 22
- Editing your profile information ......................................... 23
- Switching languages ............................................................ 24
- Enabling/disabling email notifications ................................... 24
- Report subscriptions management ....................................... 25
  - Subscribing to reports ..................................................... 25
  - Editing report subscriptions ............................................. 26
  - Sending reports from report subscriptions ....................... 27
  - Unsubscribing reports ..................................................... 27
- The user interface layout ...................................................... 27
  - Home .............................................................................. 28
  - Header ............................................................................ 28
  - Menu bar .......................................................................... 29

**Requests** ..................................................................................... 30
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up and configuring request functions</td>
<td>31</td>
</tr>
<tr>
<td>Managing shops</td>
<td>31</td>
</tr>
<tr>
<td>Displaying shops</td>
<td>32</td>
</tr>
<tr>
<td>Creating shops</td>
<td>32</td>
</tr>
<tr>
<td>Editing shops</td>
<td>33</td>
</tr>
<tr>
<td>Deleting shops</td>
<td>34</td>
</tr>
<tr>
<td>Managing shop shelves</td>
<td>35</td>
</tr>
<tr>
<td>Managing access to requestable products in shops</td>
<td>38</td>
</tr>
<tr>
<td>Managing requestable products in shops</td>
<td>40</td>
</tr>
<tr>
<td>Managing service categories</td>
<td>41</td>
</tr>
<tr>
<td>Displaying service categories</td>
<td>42</td>
</tr>
<tr>
<td>Creating service categories</td>
<td>42</td>
</tr>
<tr>
<td>Editing service categories</td>
<td>44</td>
</tr>
<tr>
<td>Deleting service categories</td>
<td>46</td>
</tr>
<tr>
<td>Managing service items</td>
<td>46</td>
</tr>
<tr>
<td>Displaying service items</td>
<td>47</td>
</tr>
<tr>
<td>Editing service items</td>
<td>47</td>
</tr>
<tr>
<td>Requesting products</td>
<td>50</td>
</tr>
<tr>
<td>Adding products to the shopping cart</td>
<td>50</td>
</tr>
<tr>
<td>Managing products in the shopping cart</td>
<td>52</td>
</tr>
<tr>
<td>Displaying the shopping cart</td>
<td>53</td>
</tr>
<tr>
<td>Removing products from the shopping cart</td>
<td>53</td>
</tr>
<tr>
<td>Setting the validity period of products in your shopping cart</td>
<td>54</td>
</tr>
<tr>
<td>Specifying the priority of products in your shopping cart</td>
<td>55</td>
</tr>
<tr>
<td>Giving reasons for requests</td>
<td>55</td>
</tr>
<tr>
<td>Checking the shopping cart</td>
<td>56</td>
</tr>
<tr>
<td>Requesting products in the shopping cart for multiple identities</td>
<td>56</td>
</tr>
<tr>
<td>Deleting shopping carts</td>
<td>57</td>
</tr>
<tr>
<td>Submitting requests</td>
<td>57</td>
</tr>
<tr>
<td>Requesting for other identities or subidentities</td>
<td>58</td>
</tr>
<tr>
<td>Displaying and requesting other identity’s products</td>
<td>59</td>
</tr>
<tr>
<td>Requesting products through reference users</td>
<td>59</td>
</tr>
<tr>
<td>Requesting products through peer groups</td>
<td>60</td>
</tr>
<tr>
<td>Requesting privileged access</td>
<td>60</td>
</tr>
<tr>
<td>Requests for Active Directory groups</td>
<td>62</td>
</tr>
</tbody>
</table>
Requesting new Active Directory groups ......................................................... 62
Requesting changes to Active Directory groups ............................................. 63
Requesting deletion of Active Directory groups .............................................. 64
Requesting new SharePoint groups ................................................................. 65
Saved for Later list ......................................................................................... 66
  Saving products for later ............................................................................... 66
  Displaying Saved for Later list ..................................................................... 67
  Requesting products on the Saved for Later list ........................................... 67
  Removing products from the Saved for Later list ......................................... 68
  Deleting the Saved for Later list .................................................................. 69
Pending requests ............................................................................................. 69
  Displaying pending requests ......................................................................... 69
  Approving and denying requests .................................................................. 70
    Approving pending requests from newly created Active Directory groups .... 71
    Approving pending requests from newly created SharePoint groups ........... 72
    Approving new managers' pending requests ............................................. 73
  Appointing other approvers for pending requests ......................................... 74
    Rerouting approvals of pending requests ................................................ 74
    Appointing additional approvers to pending requests ................................. 75
    Delegating approvals of pending requests to other identities ....................... 76
  Rejecting request approval .......................................................................... 78
Displaying request history ............................................................................ 79
Canceling requests ......................................................................................... 79
Renewing products with limit validity periods .................................................. 80
Unsubscribing products .................................................................................. 81
Displaying approvals ..................................................................................... 83
Undoing approvals ......................................................................................... 83
Attestation ....................................................................................................... 85
  Managing attestations ................................................................................... 85
  Attestation policies ....................................................................................... 86
    Displaying attestation policies .................................................................. 86
    Displaying attestation policy reports ......................................................... 87
    Setting up attestation policies ................................................................... 88
    Editing attestation policies ....................................................................... 90
    Copying attestation policies ..................................................................... 93
Deleting attestation policies .................................................................96
Starting attestation ..................................................................................96
Running sample attestations ....................................................................97
Attestation runs ........................................................................................98
Displaying attestation policy runs ............................................................98
Displaying attestors of application runs ................................................. 99
Displaying attestation cases of application runs .....................................99
Displaying attestation run reports ............................................................100
Extending attestation runs .......................................................................100
Attestation by peer group analysis ..........................................................101
Managing samples ..................................................................................101
Displaying samples ................................................................................101
Creating samples ...................................................................................102
Editing samples ......................................................................................102
Deleting samples ....................................................................................103
Sending attestation reminders .................................................................103
Sending reminders about attestation runs ..............................................103
Pending attestations ...............................................................................104
Displaying pending attestation cases ......................................................104
Granting or denying attestation cases .....................................................105
Appointing other approvers for pending attestation cases ....................106
  Rerouting approvals of pending attestation cases ...............................107
  Appointing additional approvers to pending attestation cases .......... 108
  Delegating approvals of pending attestation cases to other identities .110
Rejecting approval of attestation cases ....................................................112
Displaying attestation history .................................................................113

Compliance .............................................................................................114
Displaying compliance rules and rule violations .......................................114
Displaying reports about compliance rules and rule violations ...............115

Responsibilities .......................................................................................116
My responsibilities ...................................................................................116
  Managing my departments ....................................................................117
  Displaying my departments ...............................................................117
  Displaying and editing my department main data ................................117
Managing my department memberships ......................................................... 119
Managing my departments' entitlements ......................................................... 121
Managing my application roles ........................................................................ 123
Displaying my application roles ................................................................. 123
Displaying and editing my application roles' main data .................................. 124
Managing my application role memberships ................................................. 125
Managing my business roles .......................................................................... 128
Displaying my business roles ........................................................................ 128
Displaying and editing my business roles' main data ..................................... 129
Managing my business role memberships ..................................................... 131
Managing my business roles' entitlements ...................................................... 133
Managing my identities .................................................................................. 135
Displaying my identities .............................................................................. 135
Displaying and editing my identities' main data ............................................ 136
Displaying my identities' application roles .................................................... 138
Displaying my identities' system entitlements ................................................. 138
Displaying my identities' user accounts ........................................................ 138
Deactivating my identities ............................................................................. 139
Assigning other managers to my identities ................................................... 140
Creating reports about my identities ............................................................ 140
Managing my identities' attestation cases ...................................................... 141
Marking my identities as security risks ........................................................ 143
Creating passcodes for my identities ............................................................ 144
Managing my cost centers ............................................................................ 144
Displaying my cost centers .......................................................................... 144
Displaying and editing my cost center main data .......................................... 145
Managing my cost center memberships ........................................................ 146
Managing my cost centers' entitlements ........................................................ 149
Managing my locations .................................................................................. 151
Displaying my locations .............................................................................. 151
Displaying and editing my locations' main data .......................................... 151
Managing my location memberships ............................................................. 153
Managing my locations' entitlements ............................................................. 155
Managing my system entitlements ................................................................. 157
Displaying my system entitlements ................................................................. 157
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying and editing my system entitlements' main data</td>
<td>158</td>
</tr>
<tr>
<td>Creating reports about my system entitlements</td>
<td>159</td>
</tr>
<tr>
<td>Making my system entitlements requestable</td>
<td>160</td>
</tr>
<tr>
<td>Specifying my system entitlement owners</td>
<td>160</td>
</tr>
<tr>
<td>Managing my system entitlements' service items</td>
<td>161</td>
</tr>
<tr>
<td>Managing my system entitlement memberships</td>
<td>164</td>
</tr>
<tr>
<td>Managing my system entitlements' child groups</td>
<td>167</td>
</tr>
<tr>
<td>Managing my system entitlements' attestation cases</td>
<td>167</td>
</tr>
<tr>
<td>Managing my system roles</td>
<td>169</td>
</tr>
<tr>
<td>Displaying my system roles</td>
<td>170</td>
</tr>
<tr>
<td>Displaying and editing my system roles' main data</td>
<td>170</td>
</tr>
<tr>
<td>Managing my system role memberships</td>
<td>171</td>
</tr>
<tr>
<td>Managing my system roles' entitlements</td>
<td>174</td>
</tr>
<tr>
<td>Delegating tasks</td>
<td>175</td>
</tr>
<tr>
<td>Displaying delegations</td>
<td>176</td>
</tr>
<tr>
<td>Creating delegations</td>
<td>176</td>
</tr>
<tr>
<td>Canceling delegations</td>
<td>177</td>
</tr>
<tr>
<td>Deleting delegations</td>
<td>177</td>
</tr>
<tr>
<td>Ownerships</td>
<td>178</td>
</tr>
<tr>
<td>Assigning owners to system entitlements</td>
<td>178</td>
</tr>
<tr>
<td>Managing data</td>
<td>180</td>
</tr>
<tr>
<td>Managing identities</td>
<td>180</td>
</tr>
<tr>
<td>Displaying identities</td>
<td>181</td>
</tr>
<tr>
<td>Displaying identities' application roles</td>
<td>181</td>
</tr>
<tr>
<td>Displaying identities' system entitlements</td>
<td>182</td>
</tr>
<tr>
<td>Displaying identities' user accounts</td>
<td>182</td>
</tr>
<tr>
<td>Deactivating identities</td>
<td>182</td>
</tr>
<tr>
<td>Reactivating identities</td>
<td>183</td>
</tr>
<tr>
<td>Assigning other managers to identities</td>
<td>183</td>
</tr>
<tr>
<td>Creating reports about identities</td>
<td>183</td>
</tr>
<tr>
<td>Managing attestation cases of identities</td>
<td>184</td>
</tr>
<tr>
<td>Displaying attestation cases of identities</td>
<td>184</td>
</tr>
<tr>
<td>Approving and denying attestation cases of identities</td>
<td>185</td>
</tr>
<tr>
<td>Deleting identities</td>
<td>185</td>
</tr>
<tr>
<td>Marking identities as security risks</td>
<td>186</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Revoking identities' security risks</td>
<td>186</td>
</tr>
<tr>
<td>Displaying identity risk indexes</td>
<td>187</td>
</tr>
<tr>
<td>Managing user accounts</td>
<td>187</td>
</tr>
<tr>
<td>Displaying user accounts</td>
<td>187</td>
</tr>
<tr>
<td>Managing user account memberships</td>
<td>188</td>
</tr>
<tr>
<td>Displaying user account memberships</td>
<td>188</td>
</tr>
<tr>
<td>Creating reports about user accounts</td>
<td>188</td>
</tr>
<tr>
<td>Managing system entitlements</td>
<td>188</td>
</tr>
<tr>
<td>Displaying system entitlements</td>
<td>189</td>
</tr>
<tr>
<td>Making system entitlements requestable</td>
<td>189</td>
</tr>
<tr>
<td>Displaying and editing system entitlements main data</td>
<td>190</td>
</tr>
<tr>
<td>Specifying system entitlement owners</td>
<td>191</td>
</tr>
<tr>
<td>Managing service items for system entitlements</td>
<td>193</td>
</tr>
<tr>
<td>Creating service items for system entitlements</td>
<td>193</td>
</tr>
<tr>
<td>Editing system entitlement service items</td>
<td>196</td>
</tr>
<tr>
<td>Managing system entitlement memberships</td>
<td>199</td>
</tr>
<tr>
<td>Displaying system entitlement memberships</td>
<td>199</td>
</tr>
<tr>
<td>Analyzing assignments to system entitlements</td>
<td>199</td>
</tr>
<tr>
<td>Assigning identity system entitlements</td>
<td>200</td>
</tr>
<tr>
<td>Removing system entitlements from identities</td>
<td>201</td>
</tr>
<tr>
<td>Managing system entitlement child groups</td>
<td>201</td>
</tr>
<tr>
<td>Displaying system entitlement child groups</td>
<td>202</td>
</tr>
<tr>
<td>Managing attestation cases of system entitlements</td>
<td>202</td>
</tr>
<tr>
<td>Displaying attestation cases of system entitlements</td>
<td>202</td>
</tr>
<tr>
<td>Approving and denying attestation cases of system entitlements</td>
<td>203</td>
</tr>
<tr>
<td>Creating reports about system entitlements</td>
<td>204</td>
</tr>
<tr>
<td>Managing departments</td>
<td>204</td>
</tr>
<tr>
<td>Displaying departments</td>
<td>204</td>
</tr>
<tr>
<td>Displaying and editing department main data</td>
<td>204</td>
</tr>
<tr>
<td>Managing department memberships</td>
<td>206</td>
</tr>
<tr>
<td>Displaying department memberships</td>
<td>206</td>
</tr>
<tr>
<td>Analyzing assignments to departments</td>
<td>206</td>
</tr>
<tr>
<td>Adding identities to departments</td>
<td>207</td>
</tr>
<tr>
<td>Removing identities from departments</td>
<td>208</td>
</tr>
<tr>
<td>Managing department entitlements</td>
<td>208</td>
</tr>
</tbody>
</table>
Managing business role entitlements ................................................................. 226
Displaying business role entitlements .............................................................. 227
Adding entitlements to business roles ............................................................. 227
Deleting business role entitlements ................................................................. 227
Managing system roles ..................................................................................... 228
Displaying system roles ................................................................................... 228
Displaying and editing system role main data .................................................. 228
Managing system role memberships ................................................................. 230
Displaying system role memberships .............................................................. 230
Analyzing assignments to system roles ......................................................... 230
Assigning identities to system roles ............................................................... 231
Removing identities from my system roles ...................................................... 231
Managing system role entitlements ................................................................. 232
Displaying system role entitlements ............................................................... 232
Adding entitlements to system roles .............................................................. 232
Deleting system role entitlements ................................................................. 233

Appendix: Attestation conditions and approval policies from attestation procedures ...................................................... 234
Attesting primary departments ....................................................................... 234
Attesting primary business roles .................................................................... 235
Attesting primary cost centers ....................................................................... 236
Attesting primary locations ........................................................................... 236
Attesting secondary departments .................................................................... 237
Attesting secondary cost centers .................................................................... 238
Attesting secondary locations ........................................................................ 238
Attesting PAM asset groups ........................................................................... 239
Attesting PAM asset accounts ....................................................................... 239
Attesting PAM assets ..................................................................................... 240
Attesting PAM user groups ............................................................................ 240
Attesting PAM user accounts ........................................................................ 240
Attesting PAM account groups ...................................................................... 241
Attesting PAM directory accounts ................................................................ 242
Attesting PAM accesses ................................................................................ 243
Attesting departments .................................................................................... 244
Application role attestation .......................................................................... 244
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 14
- [Navigation and use](#) on page 16
- [Displaying the address book](#) on page 20
- [Managing password questions](#) on page 20
- [Changing passwords](#) on page 22
Logging in and out

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

| TIP: If you do not yet have an account, contact your manager. |
| NOTE: If you have forgotten your password and your account cannot be unlocked with the question-answer function, you can ask your manager for a passcode. |

Detailed information about this topic

- Logging in on page 14
- Logging in to the Password Reset Portal on page 15
- Logging off on page 16

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 22
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 14
- Logging off on page 16

Logging off

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

To log off from Web Portal

1. In the header, click ❌ (Profile) > Log Off.
2. In the Log Off dialog, confirm the prompt with Yes.
   Your logoff was successful.
   TIP: Your system may be configured to log you off automatically if you are inactive for a long period of time.

Navigation and use

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

Detailed information about this topic

- Simple navigation on page 17
- Search on page 18
- Help on page 19
- Filtering on page 20
Simple navigation

Simple commands

<table>
<thead>
<tr>
<th>Table 1: Overview of simple commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab</td>
</tr>
<tr>
<td>Enter or, if required, Space</td>
</tr>
<tr>
<td>Backspace</td>
</tr>
<tr>
<td>Alt + Left arrow or Alt + Right arrow</td>
</tr>
</tbody>
</table>

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

Go to the home page

<table>
<thead>
<tr>
<th>Table 2: Overview of key combinations for navigating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab</td>
</tr>
<tr>
<td>Shift + Tab</td>
</tr>
<tr>
<td>Enter key</td>
</tr>
</tbody>
</table>

Simple elements

<table>
<thead>
<tr>
<th>Table 3: Overview of the controls used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button</td>
</tr>
<tr>
<td>Link</td>
</tr>
<tr>
<td>Dialog window</td>
</tr>
<tr>
<td>Menu</td>
</tr>
<tr>
<td>Input field</td>
</tr>
<tr>
<td>Tiles</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sam User</td>
<td>Finds Sam User but not Sam Identity.</td>
</tr>
<tr>
<td></td>
<td>Search results must contain all of the separate terms in the query. A logical AND is used.</td>
</tr>
<tr>
<td>Sam OR Identity</td>
<td>Finds Sam User and Pat Identity.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Sam NOT User</td>
<td>Finds Sam Identity but not Sam User.</td>
</tr>
<tr>
<td></td>
<td>The results of this search do not contain the term that comes after NOT.</td>
</tr>
<tr>
<td>U*</td>
<td>Finds User1 and User2.</td>
</tr>
<tr>
<td></td>
<td>The * functions as a wildcard for any number of characters to complete the term.</td>
</tr>
<tr>
<td>Use?</td>
<td>Finds User but not User1.</td>
</tr>
<tr>
<td></td>
<td>The ? functions as a wildcard for a single character to complete the term.</td>
</tr>
<tr>
<td>&quot;Sam User&quot;</td>
<td>Provides results in which the search terms Sam and User follow one another. Results of this search contain the string in quotes as phrase.</td>
</tr>
</tbody>
</table>
Example  | Description
--- | ---
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 19

**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 \( \times \) (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 19

**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 \( \text{Help} \) >.
Filtering

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

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

To use a filter

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

Displaying the address book

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

To display the address book

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

Managing password questions

If you forget your password, you can change it at any time in the Web Portal (see Changing passwords on page 22). 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). You can reset locked password questions at any time.

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

If the Web Portal is configured accordingly, password questions are deleted after successful use.
Detailed information about this topic

- Creating password questions on page 21
- Editing password questions on page 21
- Deleting password questions on page 22

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. Click Edit.
6. Specify the following:
   - Question: Enter your question.
   - Answer: Enter the answer to your question (above).
Repeat answer: Enter the answer to your question again.

7. 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, click 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 15).

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 22), 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 20

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.

**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) > **My 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 that you want to notified about.
   
   - To disable notifications, deselect the box next to the event that you do not want to notified about any longer.
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.

Detailed information about this topic

- Subscribing to reports on page 25
- Editing report subscriptions on page 26
- Sending reports from report subscriptions on page 27
- Unsubscribing reports on page 27

Subscribing to reports

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

To add a subscription

1. In the header, click 🔄 (Profile) > My 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.
   On the Report Subscriptions page, click Add subscription.
5. In the Add Report Subscription pane, in the list, click the report that you want to subscribe to.
   TIP: To search for a specific report, in the Search field, enter the name of the report.
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) > My 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 page, click Edit next to the report subscription that you want to edit.
5. In the details pane, under Subscription Details, edit the following report subscription settings:
   
   - **Subscription:** Enter the report subscription's name.
   - **Report:** Select the report that you want to subscribe to.
   - **Schedule:** Select how often you want to receive the report (once a week, for example).
   - **Format (email attachment):** Select which format you want to receive the report in. The report is sent in this format as a file attachment in an email.
   - **Additional subscribers:** Click Assign/Change, select the check box next to the identity who will also receive this report and click Apply.
     
     **TIP:** To remove a subscription, deselect the box next to the corresponding identity. To remove all subscriptions, click Clear selection. Click Apply.
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 > My 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 to yourself, click (Actions) > Send report to me next to the subscription of the report that you want to send.
   - To send the report to all subscribers, click (Actions) > Send report to all subscribers next to the subscription of the report you want to send.

Unsubscribing reports

You can unsubscribe reports.

To unsubscribe a report

1. In the header, click Profile > My profile.
2. On the Profile Settings page, click the Report Subscriptions tab.
3. (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 28
- Header on page 28
- Menu bar on page 29

Home

Open the home page by clicking the company logo.

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

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

Header

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

Table 6: Functions in the header

<table>
<thead>
<tr>
<th>Icon</th>
<th>Use these menu items to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>- View your personal data with memberships, responsibilities, and entitlements and to edit setting (for example, your Password questions)</td>
</tr>
<tr>
<td></td>
<td>- Display your company's address book</td>
</tr>
</tbody>
</table>
- Log off
- Change the language
- Enable/disable email notifications
- Manage report subscriptions

**Help** This menu includes online help, contact to customer service and information about the connection and the product.

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

Here you can open the help. The help contains the entire contents of the Web Portal User Guide.

**Menu bar**

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

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

**To open a menu**

1. Click a menu in the menu bar.
   This expands the menu and shows more menu items.
2. Click a menu item.
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 69).
- You are notified whether your request is granted or denied.

**Detailed information about this topic**

- Setting up and configuring request functions on page 31
- Requesting products on page 50
- Saved for Later list on page 66
- Pending requests on page 69
- Displaying request history on page 79
- Canceling requests on page 79
- Renewing products with limit validity periods on page 80
- Unsubscribing products on page 81
- Displaying approvals on page 83
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 You can edit details of existing shops. on page 33 and Editing shelf details on page 37).

Detailed information about this topic

- Managing shops on page 31

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 35). Products are assigned to these shelves and can then be requested (see Managing requestable products in shops on page 40).

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

You can also decide who is able to request products from shops (see Managing access to requestable products in shops on page 38).

Detailed information about this topic

- Displaying shops on page 32
- Creating shops on page 32
- Editing shops on page 33
Deleting shops on page 34
Managing shop shelves on page 35
Managing access to requestable products in shops on page 38
Managing requestable products in shops on page 40

Displaying shops

You can display any of the shops and their details.

To display shops

1. In the menu bar click Setup > Shops.
   This opens the Shops page.
2. (Optional) To display details of a shop, in the list, click on the shop.
3. (Optional) You can perform the following actions:
   - You can see the shop’s shelves (see You can display any of the shop’s shelves and their details. on page 35).
   - You can display who can request products from the shop (see You can display the members of shops. These members can request products from the respective shop. on page 38).

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 33).

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 7: Shop main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a full, descriptive name for the shop.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the shop.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click Assign/Change and select an application role. Members of this application role can approve attestation cases affecting products that</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>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 attester.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Click Assign/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.</td>
</tr>
<tr>
<td>Owner</td>
<td>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.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>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.</td>
</tr>
</tbody>
</table>

4. Click **Create**.

5. (Optional) Create shelves for the shop (see You can create shelves for shops and identities can request system entitlements from them. on page 35). In the shelves, you can specify which products can be requested from the shop (see Adding products to shelves on page 40).

6. (Optional) To specify who can request products from the shop, add members to the shop (see You can add members to shops. These identities can then request products from the respective shop. on page 38).

### Editing shops

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

- Edit shop details (see You can edit details of existing shops. on page 33)
- Manage shop shelves (see Managing shop shelves on page 35)
- Specify who can request products from shops (see Managing access to requestable products in shops on page 38)
- Specify which products can be requested from shops (see Managing requestable products in shops on page 40)

### 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 8: Shop main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a full, descriptive name for the shop.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the shop.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click Assign/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 attester.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Click Assign/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.</td>
</tr>
<tr>
<td>Owner</td>
<td>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.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>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.</td>
</tr>
</tbody>
</table>

4. Click Save.

### Deleting shops

You can delete shops.

**NOTE:** Before you can delete a shop, you must delete all shelves from the shop (see You can delete shops. on page 37) and remove all members from the shop (see You can remove members from shops. These identities can then no longer request products from the shop. on page 39).
To delete a shop

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

Managing shop shelves

You can display, create, edit, or delete shop shelves.
Each shop contains a number of shelves from which identities can request products. There are various products available for request on shelves. Shelves are set up under each shop.

Detailed information about this topic

- You can display any of the shop's shelves and their details. [on page 35]
- You can create shelves for shops and identities can request system entitlements from them. [on page 35]
- When you edit the existing shelves of a shop, you can perform the following actions: [on page 36]
  - Editing shelf details [on page 37]
  - You can delete shops. [on page 37]

Displaying shop shelves

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

To display the shelves in a store

1. In the menu bar click Setup > Shops.
2. On the Shops page, in the list, click the shop whose shelves you want to display.
3. In the Edit Shop pane, click the Shelves tab.
4. (Optional) To display details of a shelf, click it in the list.
5. (Optional) You can display the products that can be requested over this shelf (see Displaying requestable products on page 40).

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 9: Shelves main data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a full, descriptive name for the shelf.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the shelf.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click Assign/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 attester.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Click Assign/Change and select the approval policies that control how approvers are determined if products are requested from this shelf in the Web Portal. This setting is inherited by all the products that are assigned to this shop and do not have any approval policies.</td>
</tr>
<tr>
<td>Owner</td>
<td>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.</td>
</tr>
<tr>
<td>Deputy manager</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 40).

**Editing shop shelves**

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

- Edit shelf details (see You can edit details of existing shops. on page 33)
- Specify which products can be requested from shops (see Managing requestable products in shops on page 40)
Editing shelf details

You can edit details of existing shelves.

To edit details of a shelf

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a full, descriptive name for the shelf.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the shelf.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click Assign/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 attester.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Click Assign/Change and select the approval policies that control how approvers are determined if products are requested from this shelf in the Web Portal. This setting is inherited by all the products that are assigned to this shop and do not have any approval policies.</td>
</tr>
<tr>
<td>Owner</td>
<td>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.</td>
</tr>
<tr>
<td>Deputy manager</td>
<td>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.</td>
</tr>
</tbody>
</table>

6. Click Save.

Related topics

- Managing requestable products in shops on page 40

Deleting shelves from shops

You can delete shops.
NOTE: Before you can delete a shelf, you must remove all the products from it (see Removing products from shelves on page 41).

To delete a shelf from a shop

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

Managing access to requestable 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

- You can display the members of shops. These members can request products from the respective shop. on page 38
- You can add members to shops. These identities can then request products from the respective shop. on page 38
- You can remove members from shops. These identities can then no longer request products from the shop. on page 39

Displaying shop members

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

To display members of a shop

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

Adding members to shops

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

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

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 in front of 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 You can add members to shops. These identities can then request products from the respective shop. on page 38). 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, in the list, click the Shop from which you want to remove a member.
3. In the Edit Shop pane, click the Access tab.
4. On the Access tab, in the list, select the check box next to the identity that you want to remove as a member.
5. Click Remove.
6. (Optional) If the member was assigned to the shop through a dynamic role, perform the following actions:
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 189) 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 40
- Adding products to shelves on page 40
- Removing products from shelves on page 41

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 in front of the product that you want to add to the shelf.
9. Click Apply.

Removing products from shelves

You can remove products from shelves, after which they can no longer be requested from 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 in front of the product that you want to remove from the shelf.
7. Click Remove.

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 196).

Detailed information about this topic

- Displaying service categories on page 42
- Creating service categories on page 42
- Editing service categories on page 44
- Deleting service categories on page 46
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 the details of a service category, next to the service category, click Edit.

Creating service categories

You can create service categories.

To create a service category

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

**Table 11: Service category main data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service category</td>
<td>Enter a full, descriptive name for the service category.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the service category.</td>
</tr>
<tr>
<td>Parent service category</td>
<td>To structure service categories hierarchically, click Assign/Change and then select the parent service category.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click Assign/Change and then select an application role. Members of this application role can approve attestation cases that affect the service category.</td>
</tr>
<tr>
<td>Product owners</td>
<td>Click Assign/Change and then select an application role. Members of this application role can edit the service category's main data. They can also be used as approvers in approval processes when requests for service items assigned to this service category.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Select the approval policy used to determine the approver when the service item is requested in the Web Portal.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Sort order</td>
<td>Enter the way you want the service category's service items to be sorted.</td>
</tr>
<tr>
<td>Picture</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Perform the following actions to do this:</td>
</tr>
<tr>
<td></td>
<td>1. Click Add/Change.</td>
</tr>
<tr>
<td></td>
<td>2. Select an image from your medium.</td>
</tr>
<tr>
<td>Application</td>
<td>To assign an application to a service category, select the application.</td>
</tr>
<tr>
<td>Service items</td>
<td>Specify the products can be requested through the service category.</td>
</tr>
<tr>
<td></td>
<td>Perform the following actions as well:</td>
</tr>
<tr>
<td></td>
<td>1. Click Assign/Change.</td>
</tr>
<tr>
<td></td>
<td>2. Select the check box in front of the service item you want to assign to the service category.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>TIP:</td>
<td>To remove a service item, deselect the relevant check box in front of the service item. To remove all service items, click <strong>Clear selection</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

**Editing service categories**

You can edit service items.

**To edit a service category**

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

### Table 12: Service category main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service category</td>
<td>Enter a full, descriptive name for the service category.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the service category.</td>
</tr>
<tr>
<td>Parent service category</td>
<td>To structure service categories hierarchically, click <strong>Assign/Change</strong> and then select the parent service category.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and then select an application role. Members of this application role can approve attestation cases that affect the service category.</td>
</tr>
<tr>
<td>Product owners</td>
<td>Click <strong>Assign/Change</strong> 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.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Select the approval policy used to determine the approver when the service item is requested in the Web Portal. <strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Sort order</td>
<td>Enter the way you want the service category's service items to be sorted.</td>
</tr>
</tbody>
</table>
| 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:  
  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:  
  1. Click **Assign/Change**.  
  2. Select the check box in front of the service item you want to assign to the service category. |
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 42).

- 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 44).

- 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 44).

To delete a service category

1. In the menu bar, click Setup > Service categories.
2. On the Service Categories page, next to the service category you want to delete, click Edit.
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 161
- Managing service items for system entitlements on page 193
- Displaying service items on page 47
- Editing service items on page 47

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, next to the service item, click Edit.

Editing service items

You can display all service items.

To display all service items

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service item</td>
<td>Enter a name for the service item.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the service item.</td>
</tr>
<tr>
<td>Service category</td>
<td>You can group different service items into service categories. To do this,</td>
</tr>
<tr>
<td></td>
<td>click Assign/Change and select the service category to which you want to</td>
</tr>
<tr>
<td></td>
<td>assign the service item.</td>
</tr>
<tr>
<td>Approval policy</td>
<td>Select the approval policy used to determine the approver when the service</td>
</tr>
<tr>
<td></td>
<td>item is requested in the Web.</td>
</tr>
</tbody>
</table>

For more information about service categories, see Managing service categories on page 41.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. days valid</td>
<td>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.</td>
</tr>
<tr>
<td>Web page</td>
<td>Specify the URL of a web page that contains more information about the product. Use the following format: <a href="https://www.example.com">https://www.example.com</a> or <a href="http://www.example.com">http://www.example.com</a>. This field allows you to link product descriptions in the internet or intranet to the service item.</td>
</tr>
<tr>
<td>Sort order</td>
<td>Specify how the service category is sorted.</td>
</tr>
<tr>
<td>Request property</td>
<td>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.</td>
</tr>
<tr>
<td>Functional area</td>
<td>Click Assign/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 One Identity Manager Risk Assessment Administration Guide.</td>
</tr>
<tr>
<td>Attestor</td>
<td>Click Assign/Change and then select an application role. Members of this application role can approve attestation cases that affect the service item.</td>
</tr>
<tr>
<td>Terms of use</td>
<td>Select the terms of use that the product's requester must accept.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Picture</td>
<td>Enter a picture for the service item. Users see this picture when they make a request. Perform the following actions as well: 1. Click <strong>Add/Change</strong>. 2. Select an image from your medium.</td>
</tr>
<tr>
<td>Request parameters must be defined per recipient</td>
<td>Select the check box to enter additional request properties separately for each recipient of this product, if the product is requested for different recipients in one request procedure.</td>
</tr>
<tr>
<td>Retain service item assignment on relocation</td>
<td>Select the check box if requests for this service item are 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.</td>
</tr>
<tr>
<td>Tags</td>
<td>Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.</td>
</tr>
<tr>
<td>Not requestable/Requestable</td>
<td>Set the switch to <strong>Requestable</strong> if you want to request system entitlements through the Web Portal. Set the switch to <strong>Not requestable</strong> if you do not want to request system entitlements through the Web Portal. For more information, see Making system entitlements requestable on page 189.</td>
</tr>
</tbody>
</table>
| 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.  
  * To specify members of a specific application role as product owners, perform the following under **Product owners**:
    1. Enable the **Select from roles** option.  
    2. In the **Product owner** field, click **Assign/Change**.  
    3. In the **Edit Product Owner** pane, click the appropriate application role.  
  * To specify a specific identity as the product owner,
perform the following under Product owners:
1. Enable the Select from identities option.
2. In the Identity list, select the corresponding identity.

4. Click Save.

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 50).
2. Verify the shopping cart and amend the product requests as required (see Managing products in the shopping cart on page 52).
3. Submit the request (see Submitting requests on page 57).

Detailed information about this topic

- Adding products to the shopping cart on page 50
- Managing products in the shopping cart on page 52
- Submitting requests on page 57
- Requesting products on the Saved for Later list on page 67
- Displaying and requesting other identity’s products on page 59
- Requesting for other identities or subidentities on page 58
- Requesting privileged access on page 60
- Requests for Active Directory groups on page 62

Adding products to the shopping cart

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

1. In the menu bar, click **Requests > New request.**
   
   This opens the **New Request** page and displays all the available products.

2. (Optional) To filter which products are displayed, perform one of the following actions:
   
   - In the search field, enter the name of a product you want to look for.
   - Click **Show products from service category** and then select the service category containing the products you want to display.

   The relevant products are displayed.

   **TIP:** To change the service category you have selected, click ✽ (Delete filter) next to the selected service category and then select another service category using **Show products from service category.**

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

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

3. Perform one of the following tasks:
   
   - In the tile view (.grpc)
     
     - Add a product to the shopping cart: On the tile with the product you want to request, click **Add to cart.**
     
     - Add multiple products to the shopping cart: Click the tile with the products you want to request and click **Add to cart** below the list.

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

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

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

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

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

   This opens the **Shopping Cart** page. Now, you can check the request and, if necessary, add to each product request (see Managing products in the shopping cart on page 52). Then send the request (see Submitting requests on page 57).

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

After you have added products to your shopping cart (see Adding products to the shopping cart on page 50), you can delete individual product requests from the cart, add more details to them, or perform other actions.

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

**To manage products in the shopping cart**

1. In the menu bar, click **Requests > Shopping cart**.
2. On the **Shopping Cart** page, edit the shopping cart.
   You can perform the following actions:
   - Remove products from the shopping cart (see Removing products from the shopping cart on page 53)
   - Define the validity of the products (see Setting the validity period of products in your shopping cart on page 54)
   - Change the priority of the requests (see Specifying the priority of products in your shopping cart on page 55)
   - Enter reasons for the requests (see Giving reasons for requests on page 55)
   - Check the shopping cart for invalid products and remove them (see Checking the shopping cart on page 56)
   - Request products for multiple identities (see Requesting products in the shopping cart for multiple identities on page 56)
   - Place products on the Saved for Later list (see Saving products for later on page 66)
   - Show the Saved for Later list (see Displaying Saved for Later list on page 67)
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 57).

**Related topics**

- Adding products to the shopping cart on page 50
- Submitting requests on page 57
- Saved for Later list on page 66
Displaying the shopping cart

After you have added products to your shopping cart (see Adding products to the shopping cart on page 50), 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 50
- Submitting requests on page 57

Removing products from the shopping cart

After adding added products to your shopping cart (see Adding products to the shopping cart on page 50), 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 57.

Related topics

- Adding products to the shopping cart on page 50
- Submitting requests on page 57

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 50), 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 80.

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

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

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

Related topics

- Adding products to the shopping cart on page 50
- Submitting requests on page 57
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 50), 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 50
- *Submitting requests* on page 57

Giving reasons for requests

After you have added products to your shopping cart (see *Adding products to the shopping cart* on page 50), 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 50
- *Submitting requests* on page 57
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 50
- Submitting requests on page 57

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 50), 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 58
- Adding products to the shopping cart on page 50
- Submitting requests on page 57

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 53
- Adding products to the shopping cart on page 50

Submitting requests

After you have added products to your shopping cart (see Adding products to the shopping cart on page 50), and edited and, if necessary, checked the request (see Managing products in the shopping cart on page 52), 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 56 and Removing products from the shopping cart on page 53).
Related topics

- Adding products to the shopping cart on page 50
- Managing products in the shopping cart on page 52
- Checking the shopping cart on page 56
- Removing products from the shopping cart on page 53

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 56.

To request products for other identities

1. In the menu bar, click Requests > New request.
2. On the New Request page, click Change next to the Recipient field.
3. In the Change recipient pane, in the list, select the check box next to the identity you want to request products for.
   
   **TIP:** To remove an identity from the recipient list, deselect the check box next to the identity.
4. Click Apply.
5. Add the products to the shopping cart (see Adding products to the shopping cart on page 50) that you want to request for the selected identities.
6. (Optional) Edit the shopping cart (see Managing products in the shopping cart on page 52).
7. Submit the request (see Submitting requests on page 57).

Related topics

- Requesting products in the shopping cart for multiple identities on page 56
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 56
- Requesting for other identities or subidentities on page 58

Requesting products through reference users

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

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

1. In the menu bar, click **Requests > New request**.
2. On the /New Request page, click **(Actions) > Select a reference user**.
3. In the Select Reference User dialog, click **Assign** next to the identity whose products you also want to request.
   This opens the New Request - By Reference User page that, on the Products and Organizational Structures tabs, lists the requests, memberships, and entitlements of the selected identity.
4. Add the products that you want to save for later, to the shopping cart (see Adding products to the shopping cart on page 50).
5. On the My Shopping Cart page, click **Submit**.

   | **TIP**: You can also add more products to your shopping cart and configure various settings. For more information, see **Managing products in the shopping cart** on page 52.

Related topics

- Requesting products through peer groups on page 60
- Managing products in the shopping cart on page 52
Requesting products through peer groups

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

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

To request other identities' products

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

      NOTE: The list may contain a maximum of one identity. To remove an identity from the list, clear the check box in front of the corresponding identity.
   c. Click Apply.
3. On the New Request page, click Actions > Show products other identities requested.
   This opens the New Request - By Peer Group page that, on the Products and Organizational Structures tabs, lists requests, memberships, and the peer group entitlements of the selected identity.
4. Add the products that you want to save for later, to the shopping cart (see Adding products to the shopping cart on page 50).
5. On the My Shopping Cart page, click Submit.

   TIP: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 52.

Related topics

- Requesting products through reference users on page 59
- Managing products in the shopping cart on page 52

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, click Show products from service category.
3. In the Service category pane, click Privileged access requests.
4. On the New Request page, 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.
5. Click Add to cart.
6. In the Request Details pane, expand the selected product.
7. In the PAM user account menu, select the PAM user account that you want to use for PAM access.
8. 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 Assign.
     2. In the System to access 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 Assign.
   - Remote desktop session request, SSH session request, or Telnet session request: In the System to access, select the corresponding PAM asset.
9. Perform the following actions:
   a. In the Account to access field, click Assign.
   b. In the Account for access 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 Assign.
10. (Optional) In the Comment field, enter a comment, for example, to justify why you are requesting this access.
11. 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.
12. 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.

13. Click **Apply**.
14. (Optional) Repeat the steps for all other users and access types.
15. Click **Submit**.
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 52.

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 79) 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 52

**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 62
- Requesting changes to Active Directory groups on page 63
- Requesting deletion of Active Directory groups on page 64

**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, click **Show products from service category**.
3. In the **Service category** pane, click the **Active Directory groups** service category.
4. Perform one of the following actions:
To request a new Active Directory security group, click the **New Active Directory security group** tile.

To request a new Active Directory distribution group, click the **New Active Directory distribution group** tile.

5. Click **Add to cart**.

6. In the **Request Details** pane, 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 **Assign** and select a container for the group.

7. Click **Apply**.

8. Click **Submit**.
   
   **TIP**: You can also add more products to your shopping cart and configure various settings. For more information, see **Managing products in the shopping cart** on page 52.

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

**Related topics**

- **Approving pending requests from newly created Active Directory groups** on page 71

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

   **TIP**: You can also add more products to your shopping cart and configure various settings. For more information, see Managing products in the shopping cart on page 52.
11. On the Shopping Cart page, click Submit.

Requesting deletion of Active Directory groups

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

To delete an Active Directory group

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

4. Click the **Delete Active Directory Group** tile.

5. Click **Add to cart**.

6. In the **Request Details** pane, in the **Active Directory group to delete** menu, select the Active Directory group that you want to delete.

7. Click **Apply**.

8. Click **Submit**.

   **TIP:** You can also add more products to your shopping cart and configure various settings. For more information, see *Managing products in the shopping cart* on page 52.

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 test**

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

2. On the **New Request** page, click **Show products from service category**.

3. In the **Service category** pane, click the **SharePoint groups** service category.

4. Click the **New SharePoint group** tile.

5. Click **Add to cart**.

6. 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.

7. Click **Apply**.

8. Click **Submit**.

   **TIP:** You can also add more products to your shopping cart and configure various settings. For more information, see *Managing products in the shopping cart* on page 52.

9. On the **Shopping Cart** page, click **Submit**.
Saved for Later list

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

Detailed information about this topic

- Saving products for later on page 66
- Displaying Saved for Later list on page 67
- Requesting products on the Saved for Later list on page 67
- Removing products from the Saved for Later list on page 68
- Deleting the Saved for Later list on page 69

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 67).

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 50).
2. In the menu bar, click Requests > Shopping cart.
3. On the Shopping Cart page, in the list, select the check boxes next to the products that you want to save for later.
4. Click : (Actions) > Move to Saved for Later list.
   The products are moved with all their settings to your shopping cart.

Related topics

- Managing products in the shopping cart on page 52
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 52

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 52.
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 69.

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 52
- Submitting requests on page 57
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 68.

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.
4. In the Delete Saved for Later List dialog, confirm the prompt with Yes.

Related topics

- Managing products in the shopping cart on page 52

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 69
- Approving and denying requests on page 70
- Appointing other approvers for pending requests on page 74
- Rejecting request approval on page 78

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 70).
To display pending requests

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

Approving and denying requests

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

To make an approval decision about a pending request

1. In the menu bar, click **Requests > Pending requests**.
2. (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. (Optional) On the **Approve Request/Deny Request** page, perform the following actions:
   a. In the **Reason for your decision** field, select a standard reason for your approval decision.
   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.
   
   **TIP:** By giving reasons, your approvals are more transparent and support the audit trail.
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**.

Related topics

- **Approving new managers' pending requests** on page 73
Approving pending requests from newly created Active Directory groups

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

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

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

**TIP**: By giving reasons, your approvals are more transparent and support the audit trail.
NOTE: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

6. Click Save.

Related topics

- Requesting new Active Directory groups on page 62

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

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

**NOTE**: For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

6. Click **Save**.
Related topics

- Requesting new SharePoint groups on page 65

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 140). 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. (Optional) In the Approve Request 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.
7. Click Save.

Related topics

- Assigning other managers to my identities on page 140
Appointing other approvers for pending requests

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

- **Reroute approval**
  
  You give the task of approving to another approval level (see Rerouting approvals of pending requests on page 74).

- **Appoint additional approver**
  
  You can give an another identity the task of approving (see Appointing additional approvers to pending requests on page 75). 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 78).
  
  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 76). 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 78).
  
  You can withdraw a delegation and delegate another identity. For example, if the other approver is not available.

Rerouting approvals of pending requests

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

**To reroute an approval**

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

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

Appointing additional approvers to pending requests

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

To add an additional approver

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

To add an additional approver to multiple requests

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

- Removing additional approvers of pending requests on page 76

Removing additional approvers of pending requests

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

**To withdraw a request’s additional approver**

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

**To withdraw additional approver from multiple requests**

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

Related topics

- Appointing additional approvers to pending requests on page 75

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 77).
To delegate an approval

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

To delegate approval of multiple requests

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

Related topics

- Withdrawing delegations from pending requests on page 77

Withdrawing delegations from pending requests

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

To withdraw an approval delegation

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

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

Related topics
- Delegating approvals of pending requests to other identities on page 76

Rejecting request approval

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

To reject an approval

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

To reject approval of multiple requests

1. In the menu bar, click Requests > Pending requests.
2. On the Pending Requests page, in the list, select the check boxes next to the requests that you do not want to make an approval decision about.
3. Click Actions > Reject approval.
4. In the Reject Approval, in the Reason for your decision pane, enter a reason for the rejecting.
5. Click Save.
- Appointing additional approvers to pending requests on page 75
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 20). For example, this allows you to show just pending requests (no approval decision yet made).
3. (Optional) To display details of a request, click Details next to the request whose details you want to see.

Related topics

- Canceling requests on page 79
- Renewing products with limit validity periods on page 80
- Unsubscribing products on page 81

Canceling requests

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

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

To cancel a request

1. In the menu bar, click Requests > Request History.
2. On the Request History page, click Filter.
3. In the filter context menu, check the Pending box.
4. (Optional) To control which requests are displayed, click Filter (see Filtering on page 20). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to cancel a request of another identity, in the Search field, enter the identity’s name.
6. Click Details next to the request you want to cancel.
7. In the View Request Details pane, click Cancel request.
8. In the Cancel Request pane, perform the following actions:
a. In the **Reason for your decision** field, enter a reason for the cancellation.
b. Click **Save**.

**Related topics**
- Requesting products on page 50
- Displaying request history on page 79
- Renewing products with limit validity periods on page 80
- Unsubscribing products on page 81

**Renewing products with limit validity periods**

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

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

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

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

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click **Filter**.
3. In the filter context menu, check the **Active** box.
4. (Optional) To control which requests are displayed, click **Filter** (see Filtering on page 20). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to renew a product of another identity, in the **Search** field, enter the identity's name.
6. Next to the product that you want to renew, click **Details**.
7. In the **View Request Details** pane, click **Renew product**.
8. In the **Renew Product** pane, perform the following actions:
   a. In the **Renewal date** field, enter the renewal date for the product. If the field is empty the product has unlimited availability.
   b. In the **Reason for your decision** field, enter a reason for the renewal.
   c. Click **Save**.
**To renew the validity period of multiple products**

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click **Filter**.
3. In the filter context menu, check the **Active** box.
4. (Optional) To control which requests are displayed, click **Filter** (see Filtering on page 20). 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 54
- Canceling requests on page 79
- Unsubscribing products on page 81

**Unsubscribing products**

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

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

**To unsubscribe a product**

1. In the menu bar, click **Requests > Request History**.
2. On the **Request History** page, click **Filter**.
3. In the filter context menu, check the **Active** box.
4. (Optional) To control which requests are displayed, click **Filter** (see Filtering on page 20). For example, this allows you to show just requests that you have carried out for other identities.
5. (Optional) If you want to unsubscribe a product of another identity, in the Search field, enter the identity’s name.

6. In the list, click Details next to the product that you want to unsubscribe.

7. In the View Request Details pane, click Unsubscribe product.

8. In the Unsubscribe Product pane, perform the following actions:
   a. In the Unsubscribed as from field, enter the date for unsubscribing the product. If you leave this field empty, the product is unsubscribed once you have clicked Saved.
   b. In the Reason for your decision field, enter a reason for unsubscribing.
   c. In the Additional comments about your decision field, enter extra information about unsubscribing.
   d. Click Save.

**To unsubscribe multiple products**

1. In the menu bar, click Requests > Request History.

2. On the Request History page, click Filter.

3. In the filter context menu, check the Active box.

4. (Optional) To control which requests are displayed, click Filter (see Filtering on page 20). 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 79
- Renewing products with limit validity periods on page 80
- Canceling requests on page 79
Displaying approvals

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

**To display approvals**

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

**Related topics**

- Withdrawing delegations from pending requests on page 77
- Removing additional approvers of pending requests on page 76
- Approving and denying requests on page 70
- Undoing approvals on page 83

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 \( \text{Filter} \) (see Filtering on page 20). For example, this allows you to show just pending requests (no approval decision yet made).
3. In the list, click **Details** next to the request whose the approval that you want to undo.
4. In the **View Request Details** pane, click **Undo approval decision**.
5. In the **Undo Approval Decision** dialog, perform the following actions:
   a. In the **Reason for your decision**, enter why you want to undo the approval.
   b. Click **Save**.
Related topics

- Displaying approvals on page 83
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 103
- Pending attestations on page 104
- Displaying attestation history on page 113
- Managing attestations on page 85

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 policies on page 86
- Starting attestation on page 96
- Running sample attestations on page 97
- Attestation runs on page 98
- Attestation by peer group analysis on page 101
- Managing samples on page 101

**Attestation policies**

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

**Detailed information about this topic**

- Displaying attestation policies on page 86
- Setting up attestation policies on page 88
- Editing attestation policies on page 90
- Copying attestation policies on page 93
- Deleting attestation policies on page 96
- Appendix: Attestation conditions and approval policies from attestation procedures on page 234

**Displaying attestation policies**

You can display enabled and disabled attestation policies.

**To display attestation policies**

1. In the menu bar, click **Attestation > Attestation Policies**.
   This opens the **Attestation Policies** page.
2. (Optional) To display disabled attestation policies, clear the **Activated attestation policies only** filter on the **Attestation Policies** page. To do this, click the button next to the filter (Clear filter).
Related topics
- Displaying attestation policies details on page 87

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

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

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

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

Related topics
- Displaying attestation run reports on page 100
Setting up attestation policies

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

To create a new attestation policy

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

Table 14: Attestation policy main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Specify whether the attestation policy is disabled or not. Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Completed attestation cases can be deleted once the attestation policy is disabled.</td>
</tr>
<tr>
<td>Attestation policy</td>
<td>Enter a name for the attestation policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the attestation policy.</td>
</tr>
<tr>
<td>Attestation procedure</td>
<td>Select which objects to attest with this attestation policy.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and then select the identities that can make approval decisions about attestation cases.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This field is only shown if you have selected an attestation policy in the <strong>Attestation policy</strong> menu that demands attestation by an approver (for example, <strong>Attestation by selected approvers</strong>).</td>
</tr>
<tr>
<td>Calculation schedule</td>
<td>Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.</td>
</tr>
<tr>
<td>Time required (days)</td>
<td>Specify how many days attestors have to make an approval decision about the attestation cases governed by this policy. If</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Owner</td>
<td>Select the identity that is responsible for this attestation policy. This identity can view and edit the attestation policy.</td>
</tr>
<tr>
<td>Risk index</td>
<td>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.</td>
</tr>
<tr>
<td>Compliance frameworks</td>
<td>Click <strong>Assign/Change</strong> and add a compliance framework to use. Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements. For example, internal requirements or auditing requirements.</td>
</tr>
<tr>
<td>Sample</td>
<td>Select which sampling data you want to use (see Running sample attestations on page 97).</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can only select samples that have not yet been assigned to an attestation policy.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When you select samples, you can not set conditions anymore and vice versa.</td>
</tr>
<tr>
<td>Close obsolete tasks automatically</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Approval by multi-factor authentication</td>
<td>Specify whether approvals about attestation cases governed by this attestation policy require multifactor authentication (for example Starling 2FA).</td>
</tr>
</tbody>
</table>

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

5. In the **Condition type** menu, click the condition type to use (see Appendix: Attestation conditions and approval policies from attestation procedures on page 234).  
   **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 234).

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 234

**Editing attestation policies**

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

**To edit an attestation policy**

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

2. On the **Attestation Policies** page, next to the attestation policy you want to edit, click **Edit**.

   To view disabled attestation policies, clear the **Activated attestation policies only** filter. To do this, click **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 93).

3. In the **Edit Attestation Policy** pane, edit the attestation policy's main data.
Table 15: Attestation policy main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Specify whether the attestation policy is disabled or not. Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Completed attestation cases can be deleted once the attestation policy is disabled.</td>
</tr>
<tr>
<td>Attestation policy</td>
<td>Enter a name for the attestation policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the attestation policy.</td>
</tr>
<tr>
<td>Attestation procedure</td>
<td>Select which selection to attest with this attestation policy. <strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and then select the identities that can make approval decisions about attestation cases. <strong>NOTE:</strong> This field is only shown if you have selected an attestation policy in the <strong>Attestation policy</strong> menu that demands attestation by an approver (for example, <strong>Attestation by selected approvers</strong>).</td>
</tr>
<tr>
<td>Calculation schedule</td>
<td>Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.</td>
</tr>
<tr>
<td>Time required (days)</td>
<td>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.</td>
</tr>
<tr>
<td>Owner</td>
<td>Select the identity that is responsible for this attestation policy. This identity can view and edit the attestation policy.</td>
</tr>
<tr>
<td>Risk index</td>
<td>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.</td>
</tr>
<tr>
<td>Compliance frameworks</td>
<td>Click <strong>Assign/Change</strong> and add a compliance framework to use. Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sample</td>
<td>Select which sampling data you want to use (see Running sample attestations on page 97).</td>
</tr>
<tr>
<td></td>
<td>NOTE: You can only select samples that have not yet been assigned to an attestation policy.</td>
</tr>
<tr>
<td></td>
<td>NOTE: When you select samples, you can not set conditions anymore and vice versa.</td>
</tr>
<tr>
<td>Close obsolete tasks automatically</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Approval by multi-factor authentication</td>
<td>Specify whether approvals about attestation cases governed by this attestation policy require multifactor authentication (for example Starling 2FA).</td>
</tr>
</tbody>
</table>

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 234).
   - 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 234).

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 234

**Copying attestation policies**

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

**To copy an attestation policy**

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

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

**Table 16: Attestation policy main data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Specify whether the attestation policy is disabled or not. Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Completed attestation cases can be deleted once the attestation policy is disabled.</td>
</tr>
<tr>
<td>Attestation policy</td>
<td>Enter a name for the attestation policy.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the attestation policy.</td>
</tr>
<tr>
<td>Attestation procedure</td>
<td>Select which objects to attest with this attestation policy.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Specify who can approve the attestations. Depending on which attestation procedure you selected, different approval policies are available.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and then select the identities that can make approval decisions about attestation cases.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This field is only shown if you have selected an attestation policy in the <strong>Attestation policy</strong> menu that demands attestation by an approver (for example, <strong>Attestation by selected approvers</strong>).</td>
</tr>
<tr>
<td>Calculation schedule</td>
<td>Specify how often an attestation run is started with this attestation policy. Each attestation run creates a new attestation case respectively.</td>
</tr>
<tr>
<td>Time required (days)</td>
<td>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 <strong>0</strong>.</td>
</tr>
<tr>
<td>Owner</td>
<td>Select the identity that is responsible for this attestation policy. This identity can view and edit the attestation policy.</td>
</tr>
<tr>
<td>Risk index</td>
<td>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.</td>
</tr>
<tr>
<td>Compliance frameworks</td>
<td>Click <strong>Assign/Change</strong> and add a compliance framework to use. Compliance frameworks are used for classifying attestation policies, compliance rules, and company policies according to regulatory requirements. For example, internal requirements or auditing requirements.</td>
</tr>
<tr>
<td>Sample</td>
<td>Select which sampling data you want to use (see <strong>Running sample attestations</strong> on page 97).</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can only select samples that have not yet been assigned to an attestation policy.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When you select samples, you can not set conditions</td>
</tr>
</tbody>
</table>
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](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 234).

   **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 234).

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 234

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 through a scheduled task or you can 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. On the Attestation Policies page, click Edit next to the attestation policy you want attest.
   | TIP: To display disabled attestation policies, enable the Show disabled policies.
3. In the Edit attestation policy pane, deselect the Disabled box.
4. In the **Calculation schedule** menu, specify how often an attestation run with this attestation policy is started.

   Each attestation run creates a new attestation case respectively.

5. Click **Save**.

**To start attestation for selected objects**

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

2. On the **Attestation Policies** page, next to the attestation policy that you want to start, click **(Actions) > Start attestation**.

3. In the **Start attestation** pane, perform one of the following actions:
   - To start attesting an object, click **Start attestation** next to the object.
   - To start attesting several object, select the check box in front of each object and click **Start attestation for selected**.
   - To start attesting all objects, click **Start attestation for all**.

**Related topics**

- Editing attestation policies on page 90
- Running sample attestations on page 97

**Running sample attestations**

You can perform attestations only for a subset of identities. For example, when attesting all identities would take too long. Samples contains identities that you can use to conduct such 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 ✗ next to the filter (Clear filter).

3. Next to the attestation policy you want to use for the sample attestation, click **Edit**.

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 101

**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 98
- Displaying attestors of application runs on page 99
- Displaying attestation cases of application runs on page 99
- Displaying attestation run reports on page 100
- Extending attestation runs on page 100
- Sending reminders about attestation runs on page 103

**Displaying attestation policy runs**

You can the display attestation runs of attestation policies.

**To display attestation policy runs**

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

- Sending reminders about attestation runs on page 103

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 103).

To show attestors of an attestation run

1. In the menu bar, click Attestation > Attestation runs.
2. On the Attestation Runs page, next to the attestation run whose attester you want to display, click Details.
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 Details next to the attestation run with the attestation cases you want to display.
3. In the View Attestation Run Details pane, click the Attestation cases tab.
4. (Optional) To further limit the attestation cases to be displayed, click (Filter) on the Attestation cases tab.
5. (Optional) To approve or deny an attestation case, perform the following actions in the Attestation cases tab:
   a. Select the check box in front of the attestation case that you want to approve or deny.
   b. Click Approve or Deny.
   c. In the Approve Attestation Case/Deny Attestation Case pane, enter a reason for your approval decision in the Reason for decision field.
   d. Click Save.
6. (Optional) To view more details of an attestation process, click Details next to the attestation process and refer to the View Attestation Process Details pane for the relevant information.
Related topics
- Displaying pending attestation cases on page 104
- Granting or denying attestation cases on page 105

Displaying attestation run reports

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

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

Related topics
- Displaying attestation policy reports on page 87

Extending attestation runs

You can extend attestation runs.

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

Related topics
- Sending reminders about attestation runs on page 103
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 234

Managing samples

You can perform attestations only for a subset of identities. For example, when attesting all identities would take too long. Samples contains identities that you can use to conduct such 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 97). |

Detailed information about this topic

- Displaying samples on page 101
- Creating samples on page 102
- Editing samples on page 102
- Deleting samples on page 103

Displaying samples

You can display all existing samples.
To display samples

1. In the menu bar, click Attestation > Sample data.
   This opens the Sample Data page.
2. (Optional) To view a sample’s data, click Edit next to 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 the name of the sample in the Display name field.
4. Click Continue.
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 Continue.
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 Edit next to 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 in front of 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 Edit next to the sample you want to edit.
3. In the **Edit Sample** pane, select the check box in front of 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 box, 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 103).

## 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 attester. This message is added to the reminder.
4. Click **Send reminder**.
To send a reminder to attestors of a selected attestation run

1. In the menu bar, click Attestation > Attestation runs.

2. On the Attestation Policy Runs page, click Details next to the attestation run that has the attestors you want to remind.

3. Perform one of the following actions:
   - To send a reminder to all attestors of the attestation run, in the View Attestation Run Details pane, click Send reminder to all attestors.
   - To send a reminder to specific attestors of the attestation run, in the View Attestation Run Details pane, click the Attestors tab, select the check boxes in front of the corresponding attestors and click Send reminder.

4. (Optional) In the Send Reminder pane, in the Message field, enter the message for the attester. This message is added to the reminder.

5. Click Send reminder.

Pending attestations

Attestation policies are run on a schedule and generate attestation cases. As attester, 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 104
- Granting or denying attestation cases on page 105
- Appointing other approvers for pending attestation cases on page 106
- Rejecting approval of attestation cases on page 112

Displaying pending attestation cases

As attester, 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 **Details** next to the attestation case.

4. (Optional) To display objects involved in an attestation case in detail, perform the following actions:
   - In the list, click **Details** next to the attestation case.
   - In the View Attestation Case Details pane, click **Show details** or **Download report**.

5. (Optional) To display all the identities that can approve the attestation case, perform the following actions:
   - In the list, click **Details** next to the attestation case.
   - In the View Attestation Case Details pane, click the **Workflow** tab.

**Related topics**

- Displaying attestation cases of application runs on page 99

**Granting or denying attestation cases**

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

**To approve an attestation case**

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

2. (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.
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. (Optional) In the **Approve Attestation Case/Deny Attestation Case** pane, perform the following actions:
   a. In the **Reason for your decision** field, select a standard reason for your approval decision.
   b. (Optional) In the **Additional comments about your decision** field, enter extra information about your approval decision.

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

   **NOTE:** For more detailed information about standard reasons, see the One Identity Manager IT Shop Administration Guide.

6. Click **Save**.

7. (Optional) If the approval requires multi-factor authentication, you are prompted to enter a security code. It may take a few minutes for the prompt to be displayed. Perform one of the following actions:
   - Click **Login with the Starling 2FA app** and follow the app instructions on your mobile phone.
   - Click **Send SMS** or **Phone call**, enter the security code, and click **Next**.

**Related topics**
- Displaying attestation cases of application runs on page 99

**Appointing other approvers for pending attestation cases**

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

- **Reroute approval**
  You give the task of approving to another approval level (see Rerouting approvals of pending attestation cases on page 107).

- **Appoint additional approver**
  You can give an additional identity the task of approving Appointing additional approvers to pending attestation cases on page 108). 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 112). 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 110). 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 112).
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 (Filter) and in the context menu, select the corresponding object under Object type.
   - To display attestation cases of a specific attestation policy, click Filter (Filter) and in the context menu, select the corresponding attestation policy under Attestation policy.
3. On the Pending Attestations page, click Details next to the attestation case whose approval you want to reroute.
4. In the View Attestation Case Details pane, click Reroute approval.
5. In the Reroute approval pane, in the Select approval level menu, select the approval level you want to reroute to.
6. (Optional) In the Reason for your decision field, enter a reason for rerouting.
7. Click Save.

To reroute multiple approvals

1. In the menu bar, click Attestation > Pending Attestations.
2. (Optional) On the Pending attestations page, perform one of the following actions:
   - To display attestation cases of a specific object, click Filter (Filter) and in the context menu, select the corresponding object under Object type.
   - To display attestation cases of a specific attestation policy, click Filter (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 (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, in the list, click **Details** next to the attestation case to which you want to add an additional approver.

4. In the **View Attestation Case Details** pane, click **Add attestor**.

5. In the **Add Additional Attestor** pane, in the **Additional approver** menu, select the identity that you want to act as an additional approver.

6. In the **Reason for your decision** field, select a standard reason for adding an additional approver.

7. Click **Save**.

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

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

2. (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 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 109

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 **Details** next to the attestation case to which you added an additional approver.
4. In the **View Attestation Case Details** pane, click **Withdraw additional attestor**.
5. In the **Withdraw Additional Attestor** pane, in the **Reason for your decision** pane, enter a reason for the withdrawal.
6. Click **Save**.

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

1. In the menu bar, click **Attestation > Pending Attestations**.
2. (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 attester**.

5. In the **Withdraw Additional Attester** 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 108

**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 111).

**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 Attestations** page, click **Details** next to the attestation case whose
   approval decision you want to delegate to another identity.

4. In the **View Attestation Case Details** pane, click **Delegate approval**.

5. In the **Delegate approval**, in the **Delegate to** menu, select the identity to which
   you want to delegate the approval.

6. In the **Reason for your decision** field, enter a reason for the delegation.

7. Click **Save**.

**To delegate approval of multiple attestation cases**

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

2. (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**, 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 111

**Withdrawing delegations from pending attestation case approvals**

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

**To withdraw an approval delegation**

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

2. On the **Attestation History** page, click **Details** next to the request whose approval delegation you want to withdraw.

3. In the **View Attestation Case Details** pane, click **Withdraw delegation**.

4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegation.

5. Click **Save**.

**To withdraw multiple delegations from approvals**

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

2. On the **Attestation History** page, in the list, select the check boxes next to the attestation cases whose approval delegations you want to withdraw.

3. Click (Actions) > **Withdraw delegation**.

4. In the **Withdraw Delegation** pane, in the **Reason for your decision** field, enter why you are withdrawing the approval delegations.

5. Click **Save**.
Relevant topics

- Delegating approvals of pending attestation cases to other identities on page 110

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 Details next to the attestation case that you do not want to make an approval decision about.
4. In the View Attestation Case Details pane, click Revert approval.
5. In the **Reject Approval**, in the Reason for your decision pane, enter a reason for the rejecting.
6. Click Save.

**To reject approval of multiple attestation cases**

1. In the menu bar, click Attestation > Pending Attestations.
2. (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**, in the Reason for your decision pane, enter a reason for the rejecting.
6. Click Save.
Displaying attestation history

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

To display the attestation history

1. In the menu bar, click **Attestation > Attestation history**.
   This opens the **Attestation History** page.
2. Perform one of the following actions:
   - To display attestation cases of a specific object, click ▼ (Filter) and in the context menu, select the corresponding object under **Object type**.
   - To display attestation cases of a specific attestation policy, click ▼ (Filter) and in the context menu, select the corresponding object under **Attestation policy**.
3. (Optional) To control which attestation cases are displayed, click ▼ (Filter) (see **Filtering** on page 20). For example, this allows you to show just pending attestation cases (no approval decision yet made).
4. (Optional) To display details of an attestation case, click **Details** next to the attestation case whose details you want to display.

Related topics

- **Withdrawing delegations from pending attestation case approvals** on page 111
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 employee 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 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.

Displaying compliance rules and rule violations

You can see an overview of the compliance rules and corresponding rule violations in the Web Portal. This information can help to determine gaps in your security or compliance policies and to develop attestation policies or mitigating controls. Mitigating controls are processes existing outside the One Identity Manager solution and reduce the risk of violation.
To display an overview of compliance rules and rule violations

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 compliance rules, clear the filter. To do this, click **Clear filters** on the context menu.

3. (Optional) To view more details of a compliance rule, click **Details** next to the compliance rule.

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 **Details** next to the compliance rule whose report you want to see.

4. In the **View Compliance Rule Details** pane, click **Download report**.
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 116
- Delegating tasks on page 175
- Ownerships on page 178

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 entitlements

Detailed information about this topic

- Managing my identities on page 135
- Managing my system entitlements on page 157
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 117
- Displaying and editing my department main data on page 117
- Managing my department memberships on page 119
- Berechtigungen meiner Abteilungen

Displaying my departments

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

To display departments

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments. This opens the Departments page and displays all the departments for which you are responsible.

Displaying and editing my department main data

You can edit the main data of the departments for which you are responsible.

To display and edit a department’s main data

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments.
3. On the **Departments** page, next to the department whose main data you want to show/edit, click **Edit**.

4. In the **Edit Department** pane, make your changes in the corresponding fields. You can edit the following main data.

**Table 17: Department main data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Enter a full, descriptive name for the department.</td>
</tr>
<tr>
<td>Short name</td>
<td>Enter a short name for the department.</td>
</tr>
<tr>
<td>Object ID</td>
<td>Enter a unique object ID for the department. For example, the object ID is required in SAP systems for assigning identities to departments.</td>
</tr>
<tr>
<td>Parent department</td>
<td>Click <strong>Assign/Change</strong> 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.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select the manager who is responsible for the department.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>Select an identity to act as a deputy to the department’s manager.</td>
</tr>
<tr>
<td>Additional manager</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role are responsible for the department.</td>
</tr>
<tr>
<td>Location</td>
<td>Click <strong>Assign/Change</strong> and select the location the cost center is primarily assigned to.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role can approve attestation cases for the department.</td>
</tr>
<tr>
<td>Cost center</td>
<td>Click <strong>Assign/Change</strong> and select the location the department is primarily assigned to.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the department.</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the department.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the department.</td>
</tr>
</tbody>
</table>

5. Click **Save**.
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 119
- Analyzing assignments to my departments on page 119
- Adding identities to my departments on page 120
- Removing identities from my departments on page 121

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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments.
3. On the Departments page, next to the department whose memberships you want to display, click Edit.
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 see 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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments.
3. On the Departments page, next to the department whose memberships you want to display, click Edit.
4. In the Edit Department pane, click the Memberships tab.
5. On the Memberships tab, click Secondary memberships.
6. Next to the corresponding membership, select the check box.

7. Click View assignment analysis.

Adding identities to my departments

You can assign identities to departments for which you are responsible. You do this through requests.

In addition, you can re-add members who were originally assigned through a dynamic role but were excluded by removing the exclusion.

To add an identity to a department

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments.
3. On the Departments page, next to the department you want to add an identity to, click Edit.
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 Select Identities pane, select the check box next to the identity you want to assign to the department.
8. Click Request memberships.
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 re-add an excluded member

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments.
3. On the Departments page, next to the department you want to add again, click Edit.
4. In the Edit Department pane, click the Memberships tab.
5. On the Memberships tab, click Excluded members.
6. Select the check box in front of the identity you want to add again as a member.
7. Click Remove exclusion.
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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments.
3. On the Departments page, next to the department with a membership you want to delete, click Edit.
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. In the Remove Memberships pane, click Remove memberships.
9. (Optional) If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the Specify Reason for Exclusion dialog, specify why you want to remove the member.
   b. Click Exclude members.

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 121
- Adding entitlements to my departments on page 122
- Deleting my department entitlements on page 122

Displaying my department entitlements

You can display entitlements that are assigned departments for which you are responsible.
To display entitlements

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments.
3. On the Departments page, next to the department whose entitlements you want to display, click Edit.
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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments.
3. On the Departments page, next to the department you want to add an entitlement to, click Edit.
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, 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.
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 50

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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Departments.
3. On the Departments page, next to the department whose entitlement you want to delete, click Edit.
4. In the Edit Department pane, click the Entitlements tab.
5. On the Permissions 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.

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 123
- Displaying and editing my application roles' main data on page 124
- Managing my application role memberships on page 125

Displaying my application roles

You can display all the application roles for which you are responsible.

To display application roles

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Application roles.
   This opens the Application Roles page and displays all the application roles for which you are responsible.
Displaying and editing my application roles' main data

You can edit the main data of the application roles that you are responsible for.

To display and edit an application role's main data

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Application roles.
3. On the Application Roles page, next to the application role whose main data you want to show/edit, click Edit.
4. In the Edit Application role pane, make your changes in the corresponding fields.
You can edit the following main data.

**Table 18: Main data of application roles**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application role</td>
<td>Enter a full, descriptive name for the application role.</td>
</tr>
<tr>
<td>Internal name</td>
<td>Enter a company internal name for the application role.</td>
</tr>
<tr>
<td>Parent application role</td>
<td>Click <strong>Assign/Change</strong> 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.</td>
</tr>
<tr>
<td>Manager</td>
<td>Click <strong>Assign/Change</strong> and select the manager responsible for the application role.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>Click <strong>Assign/Change</strong> and select an identity to act as a deputy to the application role’s manager.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the application role.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a comment for the application role.</td>
</tr>
<tr>
<td>Full name</td>
<td>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.</td>
</tr>
<tr>
<td>Department</td>
<td>Click <strong>Assign/Change</strong> and select a department for the application role.</td>
</tr>
<tr>
<td>Location</td>
<td>Click <strong>Assign/Change</strong> and select a location for the application role.</td>
</tr>
<tr>
<td>Cost center</td>
<td>Click <strong>Assign/Change</strong> and select a cost center for the application role.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

**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 126
- [Analyzing assignments to my application roles](#) on page 126
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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Application roles.
3. On the Application Roles page, next to the application role whose memberships you want to display, click Edit.
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 see 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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Application roles.
3. On the Application Roles page, next to the application role whose memberships you want to display, click Edit.
4. In the Edit Application role pane, click the Memberships tab.
5. On the Memberships tab, click Secondary memberships.
6. Next to the corresponding membership, select the check box.
7. Click View assignment analysis.

Assigning identities to my application roles

You can assign identities to application roles for which you are responsible. You do this through requests.

In addition, you can re-add members who were originally assigned through a dynamic role but were excluded by removing the exclusion.
To assign an identity to an application role

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Application roles.
3. On the Application Roles page, next to the application role you want to add an identity to, click Edit.
4. In the Edit Application Role pane, click the Memberships tab.
5. On the Memberships tab, click Request memberships.
6. In the Select Identities pane, select the check box next to the identity you want to assign to the application role.
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 re-add an excluded member

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Application roles.
3. On the Application Roles page, next to the application role you want to add again, click Edit.
4. In the Edit Application Role pane, click the Memberships tab.
5. On the Memberships tab, click Excluded members.
6. Select the check box in front of the identity you want to add again as a member.
7. Click Remove exclusion.

Related topics

- Requesting products on page 50

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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Application roles.
3. On the **Application Roles** page, next to the application role with a membership you want to delete, click **Edit**.
4. In the **Edit Application 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. In the **Remove Memberships** pane, click **Remove memberships**.
9. (Optional) If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the **Specify Reason for Exclusion** dialog, specify why you want to remove the member.
   b. Click **Exclude members**.

### 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 128
- Displaying and editing my business roles' main data on page 129
- Managing my business role memberships on page 131
- Managing my business roles' entitlements on page 133

### Displaying my business roles

You can display all the business roles for which you are responsible.

**To display business roles**

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Business roles**.
   This opens the **Business Roles** page and display all the business roles for which you are responsible.
Displaying and editing my business roles' main data

You can edit the main data of the business roles for which you are responsible.

To display and edit a business role's main data

1. Open the home page.
3. On the Business Roles page, next to the business role whose main data you want to show/edit, click Edit.
4. In the Edit Business Role pane, make your changes in the corresponding fields.
You can edit the following main data.

**Table 19: Business role main data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business role</td>
<td>Enter a full, descriptive name for the business role.</td>
</tr>
<tr>
<td>Short name</td>
<td>Enter a short name for the business role.</td>
</tr>
<tr>
<td>Internal name</td>
<td>Enter a company internal name for the business role.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the business role.</td>
</tr>
<tr>
<td>Role class</td>
<td>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.</td>
</tr>
<tr>
<td>Parent business role</td>
<td>Click Assign/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.</td>
</tr>
<tr>
<td>Role type</td>
<td>Select the role type of the business role. Role types are mainly used to regulate approval policy inheritance.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Click Assign/Change and select an application role. Members of the selected application role can approve requests for members of the business role.</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Click Assign/Change and select an application role. Members of the selected application role can approve requests for members of the business role.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select the manager who is responsible for the business role.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>Select an identity to act as a deputy to the business role's manager.</td>
</tr>
<tr>
<td>Additional manager</td>
<td>Click Assign/Change and select a cost center. Members of the selected application role are responsible for the department.</td>
</tr>
<tr>
<td>Employees do not inherit</td>
<td>Select this check box if you want to temporarily prevent identities from inheriting this business role.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a comment for the business role.</td>
</tr>
</tbody>
</table>

5. Click **Save**.
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 131
- Analyzing assignments to my business roles on page 131
- Assigning identities to my business roles on page 132
- Removing identities from my business roles on page 133

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. Open the home page.
3. On the Business Roles page, next to the business role whose memberships you want to display, click Edit.
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 see 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. Open the home page.
3. On the Business Roles page, next to the business role whose memberships you want to display, click Edit.
4. In the Edit Business Role pane, click the Memberships tab.
5. On the Memberships tab, click Secondary memberships.
6. Next to the corresponding membership, select the check box.
7. Click View assignment analysis.

Assigning identities to my business roles

You can assign identities to business roles for which you are responsible. You do this through requests.
In addition, you can re-add members who were originally assigned through a dynamic role but were excluded by removing the exclusion.

To assign a business role to an identity
1. Open the home page.
3. On the Business Roles page, next to the business role you want to add an identity to, click Edit.
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 Select Identities pane, select the check box next to the identity you want to assign to the business role.
8. Click Request memberships.
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 re-add an excluded member
1. Open the home page.
3. On the Business Roles page, next to the business role you want to add again, click Edit.
4. In the Edit Business Role pane, click the Memberships tab.
5. On the Memberships tab, click Excluded members.
6. Select the check box in front of the identity you want to add again as a member.
7. Click Remove exclusion.
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. Open the home page.
3. On the Business Roles page, next to the business role with a membership you want to delete, click Edit.
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. In the Remove Memberships pane, click Remove memberships.
9. (Optional) If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the Specify Reason for Exclusion dialog, specify why you want to remove the member.
   b. Click Exclude members.

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 134
- Adding entitlements to my business roles on page 134
- Deleting my business roles' entitlements on page 134
Displaying my business roles' entitlements

You can display entitlements that are assigned business roles for which you are responsible.

To display entitlements

1. Open the home page.
3. On the Business Roles page, next to the business role whose entitlements you want to display, click Edit.
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. Open the home page.
3. On the Business Roles page, next to the business role you want to add an entitlement to, click Edit.
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, 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.
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 50

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. Open the home page.
3. On the Business Roles page, next to the business role whose entitlement you want to delete, click Edit.
4. In the Edit Business Role pane, click the Entitlements tab.
5. On the Permissions 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.

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 135
- Deactivating my identities on page 139
- Reactivating my identities on page 139
- Displaying and editing my identities' main data on page 136
- Assigning other managers to my identities on page 140
- Creating reports about my identities on page 140
- Displaying my identities' application roles on page 138
- Displaying my identities' system entitlements on page 138
- Displaying my identities' user accounts on page 138
- Managing my identities' attestation cases on page 141
- Marking my identities as security risks on page 143
- Revoking my identities' security risks on page 143
- Creating passcodes for my identities on page 144

Displaying my identities

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

1. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
   This opens the Identities page and displays all the identities that report directly to you.
3. (Optional) To also display identities that report indirectly to you, deselect the Show only direct reports option.
4. (Optional) To display details of an identity, click it in the list.

Displaying and editing my identities' main data

You can edit the main data of the identities for which you are responsible.

To display and edit an identity’s main data

1. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
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>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal data</strong></td>
<td></td>
</tr>
<tr>
<td>Last name</td>
<td>Enter the identity's last name.</td>
</tr>
<tr>
<td>First name</td>
<td>Enter the identity's first name.</td>
</tr>
<tr>
<td>Middle name</td>
<td>Enter the identity's middle name.</td>
</tr>
<tr>
<td>Date of birth</td>
<td>Enter the identity's date of birth. Click the Calendar (Calendar) to do this and use the date picker to select the date of birth.</td>
</tr>
<tr>
<td>Personnel number</td>
<td>Enter the identity's personnel number.</td>
</tr>
<tr>
<td>Gender</td>
<td>In the menu, select the identity's gender.</td>
</tr>
<tr>
<td>Central user account</td>
<td>Enter the name of the identity's central user account.</td>
</tr>
<tr>
<td>Default email address</td>
<td>Enter the identity's default email address.</td>
</tr>
<tr>
<td>Resetting the password</td>
<td>Select the check box to allow password help desk staff</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>through the help desk is permitted.</td>
<td>to reset the identity’s password in the Operations Support Web Portal.</td>
</tr>
<tr>
<td>Identity does not pose a security risk/Identity poses a security risk</td>
<td>Toggle the switch to specify whether the identity poses a security risk or not (see Marking my identities as security risks on page 143).</td>
</tr>
</tbody>
</table>

**Organizational information**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary cost center</td>
<td>Click <strong>Assign/Change</strong> and select the identity’s primary cost center.</td>
</tr>
<tr>
<td>Primary department</td>
<td>Click <strong>Assign/Change</strong> and select the identity’s primary department.</td>
</tr>
<tr>
<td>External</td>
<td>Select the check box if this is an external identity.</td>
</tr>
<tr>
<td>Employee type</td>
<td>In the menu, select what type of identity this is. For example, an identity of this company or a trainee.</td>
</tr>
<tr>
<td>Entry date</td>
<td>Enter the date the identity started at the company. Click the ☀ (Calendar) and use the date picker to select the starting date.</td>
</tr>
<tr>
<td>Leaving date</td>
<td>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.</td>
</tr>
<tr>
<td>Manager</td>
<td>Shows you the identity's manager. <strong>TIP:</strong> If necessary, you can transfer the identity’s manager at a later date (see Assigning other managers to my identities on page 140).</td>
</tr>
<tr>
<td>Permanently deactivated</td>
<td>Select the check box if you want the identity to be permanently deactivated (see Deactivating my identities on page 139).</td>
</tr>
<tr>
<td>Temporarily disabled</td>
<td>Select the check box if you want to deactivate the identity only temporarily.</td>
</tr>
</tbody>
</table>

**Location information**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary location</td>
<td>Click <strong>Assign/Change</strong> and select the identity’s primary location.</td>
</tr>
<tr>
<td>Building</td>
<td>Enter the building where the identity works.</td>
</tr>
<tr>
<td>Floor</td>
<td>Enter which floor the identity works on.</td>
</tr>
<tr>
<td>Room</td>
<td>Enter the room the identity works in.</td>
</tr>
</tbody>
</table>
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. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
3. On the Identities page, click the identity whose application roles you want to display.
4. In the Edit Identity pane, click the Application Roles tab.

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. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
3. On the Identities page, click the identity whose system entitlements you want to display.
4. In the Edit Identity pane, click the System Entitlements tab.

Displaying my identities' user accounts

You can display user accounts that are assigned identities for which you are responsible.

---

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Street</td>
<td>Enter the road where the identity works.</td>
</tr>
<tr>
<td>Zip code</td>
<td>Enter the zip code of the identity's work location.</td>
</tr>
<tr>
<td>City</td>
<td>Enter the city where the identity works.</td>
</tr>
<tr>
<td>Country</td>
<td>In the menu, select the country where the identity works.</td>
</tr>
<tr>
<td>State</td>
<td>In the menu, select the state where the identity works.</td>
</tr>
</tbody>
</table>

6. Click Save.
To display an identity’s user accounts

1. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
3. On the Identities page, click the identity whose user accounts you want to display.
4. In the Edit Identity pane, click the User accounts tab.

Deactivating my identities

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

Effects of permanent deactivating an identity are:

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

To deactivate an identity

1. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
3. On the Identities page, click the identity you want to deactivate.
4. In the 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. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
3. On the Identities page, click the identity you want to activate.
4. In the Edit Identity pane, expand the Organizational information section.
5. In the **Organizational Information** pane, clear the **Permanently deactivated** check box.

6. Click **Save**.

### 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. Open the home page.
2. On the home page, click **Show** in the **My Direct Reports** tile.
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, disable 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 73). After the new manager approves this requests, the new manager is assigned.

### Related topics

- **Approving new managers’ pending requests** on page 73

### Creating reports about my identities

You can create reports about identity data.
To create a report about an identity

1. Open the home page.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity for which you want to create a report.
4. In the **Edit Identity** pane, click **Download report**.

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 attester 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 141
- Approving and denying attestation cases of my identities on page 142

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. Open the home page.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity whose attestation cases you want to display.
4. In the **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 **Details** next to the attestation case.

**Related topics**
- [Attestation](#) on page 85
- [Displaying pending attestation cases](#) on page 104

**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. Open the home page.
2. On the home page, click **Show** in the **My Direct Reports** tile.
3. On the **Identities** page, click the identity whose attestation cases you want decide approval on.
4. In the **Edit Identity** pane, click the **Attestation** tab.
5. On the **Attestation** tab, click ![Filter](#).
6. In the filter context menu, select the **Pending** option.
7. Perform one of the following actions:
   - To approve an attestation case, in the list, select the check box next to the attestation case and click **Approve** below the list.
   - To deny an attestation case, in the list, select the check box next to the attestation case and click **Deny** below the list.

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**.
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 blocked.

To mark an identity as a security risk

1. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
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 my identities' security risks

If identities that you manage have been flagged as a security risk, you can remove this flag again. Then the affected identity regains access to user accounts and resources.

To revoke an identity's security risk

1. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
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.
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. Open the home page.
2. On the home page, click Show in the My Direct Reports tile.
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.

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 144
- Displaying and editing my cost center main data on page 145
- Managing my cost center memberships on page 146
- Managing my cost centers' entitlements on page 149

Displaying my cost centers

You can display all the cost centers for which you are responsible.

To display cost centers

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Cost centers.
This opens the Cost Centers page and displays all the cost centers for which you are responsible.

**Displaying and editing my cost center main data**

You can edit the main data of the cost centers for which you are responsible.

*To display and edit a cost center's main data*

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Cost centers.
3. On the Cost Centers page, next to the cost center whose main data you want to show/edit, click Edit.
4. In the Edit Cost Center pane, make your changes in the corresponding fields.
You can edit the following main data.

**Table 21: Cost center main data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost center</td>
<td>Enter a full, descriptive name for the cost center.</td>
</tr>
<tr>
<td>Short name</td>
<td>Enter a short name for the cost center.</td>
</tr>
<tr>
<td>Parent cost center</td>
<td>Click <strong>Assign/Change</strong> 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.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select the manager who is responsible for the cost center.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>Select an identity to act as a deputy to the cost center's manager.</td>
</tr>
<tr>
<td>Additional manager</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role are responsible for the department.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role can approve attestation cases for the cost center.</td>
</tr>
<tr>
<td>Department</td>
<td>Click <strong>Assign/Change</strong> and select the department that the cost center is primarily assigned to.</td>
</tr>
<tr>
<td>Location</td>
<td>Click <strong>Assign/Change</strong> and select the location the cost center is primarily assigned to.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the cost center.</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the cost center.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the cost center.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

**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 147
- Analyzing assignments to my cost centers on page 147
- Adding identities to my cost centers on page 148
- Removing identities from my cost centers on page 149

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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Cost centers.
3. On the Cost Centers page, next to the cost center whose memberships you want to display, click Edit.
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 see 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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Cost centers.
3. On the Cost Centers page, next to the cost center whose memberships you want to display, click Edit.
4. In the Edit Cost Center pane, click the Memberships tab.
5. On the Memberships tab, click Secondary memberships.
6. Next to the corresponding membership, select the check box.
7. Click View assignment analysis.
Adding identities to my cost centers

You can assign identities to cost centers for which you are responsible. You do this through requests.

In addition, you can re-add members who were originally assigned through a dynamic role but were excluded by removing the exclusion.

To add an identity to a cost center

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Cost centers.
3. On the Cost Centers page, next to the cost center you want to add an identity to, click Edit.
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 Select Identities pane, select the check box next to the identity you want to assign to the cost center.
8. Click Request memberships.
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 re-add an excluded member

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Cost centers.
3. On the Cost Centers page, next to the cost center you want to add again, click Edit.
4. In the Edit Cost Center pane, click the Memberships tab.
5. On the Memberships tab, click Excluded members.
6. Select the check box in front of the identity you want to add again as a member.
7. Click Remove exclusion.

Related topics

- Requesting products on page 50
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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Cost centers.
3. On the Cost Centers page, next to the cost center with a membership you want to delete, click Edit.
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. In the Remove Memberships pane, click Remove memberships.
9. (Optional) If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the Specify Reason for Exclusion dialog, specify why you want to remove the member.
   b. Click Exclude members.

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 149
- Adding entitlements to my cost centers on page 150
- Deleting my cost center entitlements on page 150

Displaying my cost center entitlements

You can display entitlements that are assigned cost centers for which you are responsible.
To display entitlements

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Cost centers.
3. On the Cost Centers page, next to the cost center whose entitlements you want to display, click Edit.
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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click Cost centers.
3. On the Cost Centers page, next to the cost center you want to add an entitlement to, click Edit.
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, 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.
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 50

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. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Cost centers**.
3. On the **Cost Centers** page, next to the cost center whose entitlement you want to delete, click **Edit**.
4. In the **Edit Cost Center** pane, click the **Entitlements** tab.
5. On the **Permissions** 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.

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 151
- Displaying and editing my locations' main data on page 151
- Managing my location memberships on page 153
- Managing my locations' entitlements on page 155

Displaying my locations

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

To display locations

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **Locations**.
   
   This opens the **Locations** page and displays all the locations for which you are responsible.

Displaying and editing my locations' main data

You can edit the main data of the locations for which you are responsible.
To display and edit a location’s main data

1. Open the home page.
3. On the Locations page, next to the location whose main data you want to show/edit, click Edit.
4. In the Edit Location pane, make your changes in the corresponding fields.
   You can edit the following main data.

Table 22: Location main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Enter a full, descriptive name for the location.</td>
</tr>
<tr>
<td>Short name</td>
<td>Enter a short name for the location.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter an additional description for the location.</td>
</tr>
<tr>
<td>Parent location</td>
<td>Click <strong>Assign/Change</strong> 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.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select the manager who is responsible for the location.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>Select an identity to act as a deputy to the location's manager.</td>
</tr>
<tr>
<td>Additional manager</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role are responsible for the location.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role can approve attestation cases for the location.</td>
</tr>
<tr>
<td>Department</td>
<td>Click <strong>Assign/Change</strong> and select the department the location is primarily assigned to.</td>
</tr>
<tr>
<td>Cost center</td>
<td>Click <strong>Assign/Change</strong> and select the cost center the location is primarily assigned to.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the location.</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the location.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the location.</td>
</tr>
</tbody>
</table>

5. Click Save.
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 153
- Analyzing assignments to my locations on page 153
- Adding identities to my locations on page 154
- Removing identities from my locations on page 155

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. Open the home page.
3. On the Locations page, next to the location whose memberships you want to display, click Edit.
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 see 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. Open the home page.
3. On the Locations page, next to the location whose memberships you want to display, click Edit.
4. In the Edit Location pane, click the Memberships tab.
5. On the Memberships tab, click Secondary memberships.
6. Next to the corresponding membership, select the check box.
7. Click View assignment analysis.

Adding identities to my locations

You can assign identities to locations for which you are responsible. You do this through requests.

In addition, you can re-add members who were originally assigned through a dynamic role but were excluded by removing the exclusion.

To add an identity to a location

1. Open the home page.
3. On the Locations page, next to the location you want to add an identity to, click Edit.
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 Select Identities pane, select the check box next to the identity you want to assign to the location.
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 re-add an excluded member

1. Open the home page.
3. On the Locations page, next to the location you want to add again, click Edit.
4. In the Edit Location pane, click the Memberships tab.
5. On the Memberships tab, click Excluded members.
6. Select the check box in front of the identity you want to add again as a member.
7. Click Remove exclusion.

Related topics

- Requesting products on page 50
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. Open the home page.
3. On the Locations page, next to the location with a membership you want to delete, click Edit.
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. In the Remove Memberships pane, click Remove memberships.
9. (Optional) If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the Specify Reason for Exclusion dialog, specify why you want to remove the member.
   b. Click Exclude members.

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 155
- Adding entitlements to my locations on page 156
- Deleting my locations' entitlements on page 156

Displaying my locations' entitlements

You can display entitlements that are assigned locations for which you are responsible.
To display entitlements

1. Open the home page.
3. On the Locations page, next to the location whose entitlements you want to display, click Edit.
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. Open the home page.
3. On the Locations page, next to the location you want to add an entitlement to, click Edit.
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, 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 50

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. Open the home page.
3. On the Locations page, next to the location whose entitlement you want to delete, click Edit.
4. In the Edit Locations pane, click the Entitlements tab.
5. On the Permissions 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.

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 157
- Displaying and editing my system entitlements’ main data on page 158
- Creating reports about my system entitlements on page 159
- Making my system entitlements requestable on page 160
- Managing my system entitlements’ service items on page 161
- Managing my system entitlement membership on page 164
- Managing my system entitlements’ child groups on page 167
- Managing my system entitlements’ attestation cases on page 167

Displaying my system entitlements

You can display all the system entitlements for which you are responsible.
**To display system entitlements**

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, click **System entitlements**. This opens the **System Entitlements** page and displays all the system entitlements for which you are responsible.

**Displaying and editing my system entitlements' main data**

You can edit the main data of the system entitlements for which you are responsible.

**To display and edit a system entitlement's main data**

1. Open the home page.
2. On the Home page, in the **My Responsibilities** tile, 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, make your changes in the corresponding fields.
You can edit the following main data.

Table 23: System entitlement main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a full, descriptive name for the system entitlement.</td>
</tr>
<tr>
<td>Canonical name</td>
<td>Shows the automatically generated canonical name of the system entitlement.</td>
</tr>
<tr>
<td>Distinguished name</td>
<td>Shows the automatically generated distinguished name of the system entitlement.</td>
</tr>
<tr>
<td>Display name</td>
<td>Enter a name for displaying the system entitlement in the One Identity Manager tools.</td>
</tr>
<tr>
<td>Notes domain</td>
<td>Shows the Notes domain name.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the system entitlement.</td>
</tr>
<tr>
<td>Category</td>
<td>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.</td>
</tr>
<tr>
<td>IT shop</td>
<td>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 granted through a defined approval process. The system entitlement can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the One Identity Manager IT Shop Administration Guide.</td>
</tr>
<tr>
<td>Only use in IT Shop</td>
<td>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 granted using a defined approval process. The system entitlement may not be assigned directly to hierarchical roles.</td>
</tr>
</tbody>
</table>

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. Open the home page.
3. On the **System Entitlements** page, click the system entitlement for which you want to create a report.

4. In the **Edit Details** pane, click **Download report**.

**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 161).
- The system entitlement must be assigned to a shelf in a shop (see Adding products to shelves on page 40).
- The system entitlement must be marked as requestable (see following step-by-step).

**To make a system entitlement requestable**

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

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

**Related topics**

- Managing shops on page 31
- Managing my system entitlements’ service items on page 161
- Adding products to shelves on page 40

**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. Open the home page.
3. On the System Entitlements page, click the system entitlement whose owners you want to specify.
4. In the Edit System Entitlement 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 under Product owners:
     1. Enable the Select from roles option.
     2. In the Product owner field, click Assign/Change.
     3. In the Edit Product Owner pane, click the appropriate application role.
   - To specify a specific identity as the product owner, perform the following under Product owners:
     1. 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 are assigned to corresponding service items. Then you can assign these service items to a shop (see Managing requestable products in shops on page 40).

Detailed information about this topic

- Specifying my system entitlement owners on page 160
- Editing my system entitlements' service items on page 161

Editing my system entitlements' service items

You can edit the main data of service items.

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

1. Open the home page.
3. On the System Entitlements page, click the system entitlement whose service item you want to edit.
4. In the **Edit System Entitlement** pane, click the **Details** tab.
5. On the **Service Item** tab, edit the service item's main data.

### Table 24: Main data of system entitlement service items

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service item</td>
<td>Enter a name for the service item.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the service item.</td>
</tr>
<tr>
<td>Service category</td>
<td>You can group different service items into service categories. To do this, click <strong>Assign/Change</strong> and select the service category to which you want to assign the service item. For more information about service categories, see <a href="#">Managing service categories</a> on page 41.</td>
</tr>
<tr>
<td>Approval policy</td>
<td>Select the approval policy used to determine the approver when the service item is requested in the Web Portal.</td>
</tr>
<tr>
<td>Max. days valid</td>
<td>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.</td>
</tr>
<tr>
<td>Web page</td>
<td>Specify the URL of a web page that contains more information about the product. Use the following format: <a href="https://www.example.com">https://www.example.com</a> or <a href="http://www.example.com">http://www.example.com</a>. This field allows you to link product descriptions in the internet or intranet to the service item.</td>
</tr>
<tr>
<td>Sort order</td>
<td>Specify how the service category is sorted.</td>
</tr>
<tr>
<td>Request property</td>
<td>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</td>
</tr>
</tbody>
</table>
**Property** | **Description**
--- | ---
when requesting a product. |  
Functional area | Click **Assign/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 *One Identity Manager Risk Assessment Administration Guide*.  
Attestor | Click **Assign/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.  
Picture | Enter a picture for the service item. Users see this picture when they make a request. Perform the following actions as well:  
1. Click **Add/Change**.  
2. Select an image from your medium.  
Request parameters must be defined per recipient | Select the check box to enter additional request properties separately for each recipient of this product, if the product is requested for different recipients in one request procedure.  
Retain service item assignment on relocation | Select the check box if requests for this service item are 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 system entitlements through the Web Portal. Set the switch to **Not requestable** if you do not want to request system entitlements through the Web Portal. For more information, see *Making system entitlements requestable* on page 189.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product owner</td>
<td>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.</td>
</tr>
</tbody>
</table>
|                     | • To specify members of a specific application role as product owners, perform the following under **Product owners**:  
  1. Enable the **Select from roles** option.  
  2. In the **Product owner** field, click **Assign/Change**.  
  3. In the **Edit Product Owner** pane, click the appropriate application role.  
• To specify a specific identity as the product owner, perform the following under **Product owners**:  
  1. Enable the **Select from identities** option.  
  2. In the **Identity** list, select the corresponding identity.                                                                 |

6. Click **Save**.

**Related topics**

• Assigning owners to system entitlements on page 178

**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 165
• Analyzing assignments to my system entitlements on page 165
• Assigning identities to my system entitlements on page 165
• Removing identities from my system entitlements on page 166
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

1. Open the home page.
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 see 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. Open the home page.
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. Next to the appropriate membership, click View assignment analysis.

Assigning identities to my system entitlements

You can assign identities to system entitlements for which you are responsible. You do this through requests.

To assign a system entitlement to an identity

1. Open the home page.
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 **Select Identities** pane, select the check box next to the identity you want to assign to the system entitlement.

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.

**To re-add an excluded member**

1. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, click .

3. In the pane, click the **Memberships** tab.

4. On the **Memberships** tab, click **Excluded members**.

5. Select the check box in front of the identity you want to add again as a member.

6. Click **Remove exclusion**.

**Related topics**

- Requesting products on page 50

**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. Open the home page.

2. On the Home page, in the **My Responsibilities** tile, 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 Delete.
• If it is an indirect assignment, click Unsubscribe.

NOTE: You can only unsubscribe memberships that you have requested yourself.

8. In the Delete 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 167

Display my system entitlements' child groups

You can see 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. Open the home page.
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.

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

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 168
- Approving and denying my system entitlements' attestation cases on page 168

**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. Open the home page.
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 Details next to the attestation case.

**Related topics**

- Attestation on page 85
- Displaying pending attestation cases on page 104

**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. Open the home page.
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 \( \text{Filter} \).
6. In the filter context menu, select the Pending option.
7. Perform one of the following actions:
   - To approve an attestation case, in the list, select the check box next to the attestation case and click Approve below the list.
   - To deny an attestation case, in the list, select the check box next to the attestation case and click Deny below the list.
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 85
- Granting or denying attestation cases on page 105

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. Employees 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 170
- Displaying and editing my system roles' main data on page 170
- Managing my system role memberships on page 171
- Managing my system roles' entitlements on page 174

Displaying my system roles

You can display all the system roles for which you are responsible.

To display system roles

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click System roles.
   This opens the System Roles page and displays all the system roles for which you are responsible.

Displaying and editing my system roles' main data

You can edit the main data of the system roles for which you are responsible.

To display and edit a system role’s main data

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click System roles.
3. On the System Roles page, next to the system role whose main data you want to show/edit, click Edit.
4. In the Edit System Role pane, make your changes in the corresponding fields.
You can edit the following main data.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System role</td>
<td>Enter a full, descriptive name for the system role.</td>
</tr>
<tr>
<td>Display name</td>
<td>Enter a name for displaying the system role in the One Identity Manager tools.</td>
</tr>
<tr>
<td>Internal product name</td>
<td>Enter a company internal name for the system role.</td>
</tr>
<tr>
<td>System role type</td>
<td>Select the role type of the system role. The system role type specifies which type of company resources make up the system role.</td>
</tr>
<tr>
<td>Service item</td>
<td>Shows you the associated service item.</td>
</tr>
<tr>
<td>System role manager</td>
<td>Click <strong>Change</strong> and select the identity responsible for the system role. 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.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a comment for the system role.</td>
</tr>
<tr>
<td>IT shop</td>
<td>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 the request granted by a defined approval process. The system role can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the <em>One Identity Manager IT Shop Administration Guide</em>.</td>
</tr>
<tr>
<td>Only use in IT Shop</td>
<td>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 the request granted by a defined approval process. The system role may not be assigned directly to hierarchical roles.</td>
</tr>
</tbody>
</table>

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 172
- Analyzing assignments to my system roles on page 172
- Assigning identities to my system roles on page 172
- Removing identities from my system roles on page 173

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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click System roles.
3. On the System Roles page, next to the system role whose memberships you want to display, click Edit.
4. In the Edit System Role pane, click the Memberships tab.

Analyzing assignments to my system roles

You can see 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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click System roles.
3. On the System Roles page, next to the system role whose memberships you want to display, click Edit.
4. In the Edit System Role pane, click the Memberships tab.
5. On the Memberships tab, select the check box next to the corresponding membership.
6. Click View assignment analysis.

Assigning identities to my system roles

You can assign identities to system roles for which you are responsible. You do this through requests.
To assign a system role to an identity

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click System roles.
3. On the System Roles page, next to the system role you want to add an identity to, click Edit.
4. In the Edit System Role pane, click the Memberships tab.
5. On the Memberships tab, click Request memberships.
6. In the Select Identities pane, select the check box next to the identity you want to assign to the system role.
7. Click Request memberships.
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.

To re-add an excluded member

1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click .
3. In the pane, click the Memberships tab.
4. On the Memberships tab, click Excluded members.
5. Select the check box in front of the identity you want to add again as a member.
6. Click Remove exclusion.

Related topics

- Requesting products on page 50

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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click System roles.
3. On the System Roles page, next to the system role with a membership you want to delete, click Edit.
4. In the Edit System 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. In the Remove Memberships pane, click Remove 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 174
- Adding entitlements to my system roles on page 174
- Deleting my system roles' entitlements on page 175

Displaying my system roles' entitlements

You can display entitlements that are assigned system roles for which you are responsible.

To display entitlements
1. Open the home page.
2. On the Home page, in the My Responsibilities tile, click System roles.
3. On the System Roles page, next to the system role whose entitlements you want to display, click Edit.
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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click System roles.
3. On the System Roles page, next to the system role you want to add an entitlement to, click Edit.
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, 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.
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 50

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. Open the home page.
2. On the Home page, in the My Responsibilities tile, click System roles.
3. On the System Roles page, next to the system role whose entitlement you want to delete, click Edit.
4. In the Edit System Role pane, click the Entitlements tab.
5. On the Permissions 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.

Delegating tasks

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

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

Role memberships and responsibilities can also be delegated to you.

| NOTE: | In the Web Portal, a delegation is treated like a request. |
Detailed information about this topic

- Displaying delegations on page 176
- Creating delegations on page 176
- Canceling delegations on page 177
- Deleting delegations on page 177

Displaying delegations

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

To display delegations

1. In the menu bar, click Requests > Request History.
2. On the Request History page, click \( \text{(Filter)} \).
3. In the filter context menu, select the My delegations check box.
4. (Optional) To see more details of a delegation, click Details next to 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 177) 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 177).

**To cancel a delegation**

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

### Deleting delegations

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

**NOTE**: You can only delete delegations as long as they have the **Assigned** status. You can cancel delegations that have the **Request** or **Approved** status (see Canceling delegations on page 177).
To delete a delegation

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

Ownerships

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

Detailed information about this topic

- Assigning owners to system entitlements on page 178

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 assume ownership 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 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 104**).
Managing data

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

- Identities
- User accounts
- System entitlements
- Departments
- Locations
- Cost centers
- Business roles
- System roles

Detailed information about this topic

- Managing identities on page 180
- Managing user accounts on page 187
- Managing system entitlements on page 188
- Managing departments on page 204
- Managing locations on page 210
- Managing cost centers on page 216
- Managing business roles on page 222
- Managing system roles on page 228

Managing identities

You can use the Web Portal to manage identities.
Detailed information about this topic

- Displaying identities on page 181
- Displaying identities' application roles on page 181
- Displaying identities' system entitlements on page 182
- Displaying identities' user accounts on page 182
- Managing attestation cases of identities on page 184
- Assigning other managers to identities on page 183
- Deactivating identities on page 182
- Reactivating identities on page 183
- Deleting identities on page 185
- Creating reports about identities on page 183
- Marking identities as security risks on page 186

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

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 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 Application Roles tab.
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 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 **System Entitlements** tab.

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 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 **User accounts** tab.

Deactivating identities

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

Effects of permanent deactivating an identity are:

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

**To deactivate an identity**
1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **Identities**.
3. On the **Identities** page, click the identity you want to deactivate.
4. In the **Edit Identity** pane, set the switch to **Deactivated**.
5. Click **Save**.

**Reactivating identities**

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

**To reactivate an identity**

1. In the menu bar click **Data 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, set the switch to **Activated**.
5. Click **Save**.

**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 navigation, 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, perform one of the following actions:
   - In the **Manager** menu, click the manager you want to assign to the identity.
   - To remove the current manager, click **X** (**Remove assignment**).
5. Click **Save**.

**Related topics**

- **Datenprobleme anzeigen und beheben**

**Creating reports about identities**

You can create reports about identity data.
To create a report about 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 for which you want to create a report.
4. In the Edit Identity, click Download report.

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 184
- Approving and denying attestation cases of identities on page 185

Displaying attestation cases of identities

You can see 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 Details next to the attestation case.

Related topics

- Attestation on page 85
- Displaying pending attestation cases on page 104
Approving and denying attestation cases of identities

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

To approve an attestation case

1. In the menu bar click Data administration > Data Explorer.
2. In the Data Explorer navigation, click Identities.
3. In the list, click the identity whose attestation cases you want to decide approval on.
4. In the Edit Identity pane, click the Attestation tab.
5. On the Attestation tab, click Filter.
6. In the filter context menu, select the Pending option.
7. Perform one of the following actions:
   - To approve an attestation case, in the list, select the check box next to the attestation case and click Approve below the list.
   - To deny an attestation case, in the list, select the check box next to the attestation case and click Deny below the list.
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 85
- Granting or denying attestation cases on page 105

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 navigation, click Identities.
3. On the Identities page, click the identity you want to delete.
4. In the Edit Identity pane, click Delete.
5. In the Delete Identity dialog, confirm the prompt with Yes.

Marking identities as security risks

You can mark identities as a security risk. Then the user accounts and resources of the affected identity are blocked.

To mark an identity as a security risk

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 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 flagged as a security risk, you can remove this flag 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 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.
Displaying identity risk indexes

You can see identities risk indexes.

NOTE: For more detailed information about risk assessment, see the One Identity Manager Risk Assessment Administration Guide.

To display 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.
4. In the Edit Identity pane, click (Actions) > Analyze risks.

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 permissions required for accessing target system resources through its memberships in 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 187
- Displaying user account memberships on page 188

Displaying user accounts

You can see 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 Data Explorer navigation click User accounts.
   This opens the User accounts page and displays all the user accounts.
3. (Optional) To display details of a user account, click it in the list.
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 188

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. In the list, click the user account whose memberships you want to display.
4. In the Edit User Account pane, click the Memberships tab.
   TIP: If you click a system entitlement in the list, you will see more information and options (see Managing system entitlements on page 188).

Creating reports about user accounts

You can create reports about user account data.

To create a report about a user account
1. In the menu bar click Data administration > Data Explorer.
2. In the Data Explorer navigation, click Identities.
3. On the User Accounts page, click the user account for which you want to create a report.
4. In the Edit User Account, click Download report.

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 189
- Creating reports about system entitlements on page 204
- Editing system entitlement service items on page 196
- Managing system entitlement memberships on page 199
- Managing system entitlement child groups on page 201
- Managing attestation cases of system entitlements on page 202
- Making system entitlements requestable on page 189

Displaying system entitlements

You can see 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 Data Explorer navigation click **System entitlements**.
   This opens the **System Entitlements** page and displays all the system entitlements.
3. (Optional) To display details of a system entitlement, click it in the list.

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 193).
- The system entitlement must be assigned to a shelf in a shop (see Adding products to shelves on page 40).
- 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 Data Explorer navigation, click **System entitlements**.
3. (Optional) To display only those system entitlements only that are not marked as requestable, perform the following actions:
   a. Click \(\text{Filter}\).
   b. In the filter context menu, select the \textbf{Not requestable} check box.
4. In the list, select the check box in front of the system entitlement that you want to make requestable.
5. Under the list, set the switch to \textbf{Make selected items requestable} and click \textbf{Update}.

\text{TIP:} If you do not want the system entitlement to be requested in the Web Portal anymore, set the switch to \textbf{Make selected items not requestable}.

**Related topics**

- Managing shops on page 31
- Managing service items for system entitlements on page 193
- Adding products to shelves on page 40

**Displaying and editing system entitlements main data**

You can see and edit system entitlements' main data.

\textit{To display and edit a system entitlement's main data}

1. In the menu bar click \textbf{Data administration} > \textbf{Data Explorer}.
2. In the Data Explorer navigation, click \textbf{System entitlements}.
3. On the \textbf{System Entitlements} page, click the system entitlement whose main data you want to display.
4. In the **Edit System Entitlement** pane, make your changes in the relevant fields.

### Table 26: System entitlement main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a full, descriptive name for the system entitlement.</td>
</tr>
<tr>
<td>Canonical name</td>
<td>Shows the automatically generated canonical name of the system entitlement.</td>
</tr>
<tr>
<td>Distinguished name</td>
<td>Shows the automatically generated distinguished name of the system entitlement.</td>
</tr>
<tr>
<td>Display name</td>
<td>Enter a name for displaying the system entitlement in the One Identity Manager tools.</td>
</tr>
<tr>
<td>Notes domain</td>
<td>Shows the Notes domain name.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the system entitlement.</td>
</tr>
<tr>
<td>Category</td>
<td>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.</td>
</tr>
<tr>
<td>IT shop</td>
<td>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 granted through a defined approval process. The system entitlement can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the One Identity Manager IT Shop Administration Guide.</td>
</tr>
<tr>
<td>Only use in IT Shop</td>
<td>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 granted using a defined approval process. The system entitlement may not be assigned directly to hierarchical roles.</td>
</tr>
</tbody>
</table>

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 Data Explorer navigation, click System entitlements.
3. On the System Entitlements page, click the system entitlement whose owners you want to specify.
4. In the Edit System Entitlement 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 under Product owners:
     1. Enable the Select from roles option.
     2. In the Product owner field, click Assign/Change.
     3. In the Edit Product Owner pane, click the appropriate application role.
   - To specify a specific identity as the product owner, perform the following under Product owners:
     1. 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 under Product owners:
     1. Enable the Select from roles option.
     2. In the Product owner field, click Assign/Change.
     3. In the Edit Product Owner pane, click the appropriate application role.
   - To specify a specific identity as the product owner, perform the following under Product owners:
     1. 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 are assigned to corresponding service items. Then you can assign these service items to a shop (see Managing requestable products in shops on page 40).

Detailed information about this topic

- Creating service items for system entitlements on page 193
- Specifying system entitlement owners on page 191
- Editing system entitlement service items on page 196

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 Entitlements area, click the Details tab.
5. On the Details tab, click Create service item.
6. Click Service Item tab.
7. On the Service Item tab, edit the service item's main data.

Table 27: Main data of system entitlement service items

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service item</td>
<td>Enter a name for the service item.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the service item.</td>
</tr>
<tr>
<td>Service category</td>
<td>You can group different service items into service categories. To do this, click Assign/Change and select the service category to which you want to assign the service item. For more information about service categories, see Managing service categories on page 41.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Approval policy</td>
<td>Select the approval policy used to determine the approver when the service item is requested in the Web Portal.</td>
</tr>
<tr>
<td>Max. days valid</td>
<td>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.</td>
</tr>
<tr>
<td>Web page</td>
<td>Specify the URL of a web page that contains more information about the product. Use the following format: <a href="https://www.example.com">https://www.example.com</a> or <a href="http://www.example.com">http://www.example.com</a>. This field allows you to link product descriptions in the internet or intranet to the service item.</td>
</tr>
<tr>
<td>Sort order</td>
<td>Specify how the service category is sorted.</td>
</tr>
<tr>
<td>Request property</td>
<td>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.</td>
</tr>
<tr>
<td>Functional area</td>
<td>Click Assign/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 One Identity Manager Risk Assessment Administration Guide.</td>
</tr>
<tr>
<td>Attestor</td>
<td>Click Assign/Change and then select an application role. Members of this application role can approve attestation cases that affect the service item.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Terms of use</td>
<td>Select the terms of use that the product's requester must accept.</td>
</tr>
</tbody>
</table>
| Picture | Enter a picture for the service item. Users see this picture when they make a request. Perform the following actions as well:  
1. Click Add/Change.  
2. Select an image from your medium. |
| Request parameters must be defined per recipient | Select the check box to enter additional request properties separately for each recipient of this product, if the product is requested for different recipients in one request procedure. |
| Retain service item assignment on relocation | Select the check box if requests for this service item are 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 system entitlements through the Web Portal.  
Set the switch to Not requestable if you do not want to request system entitlements through the Web Portal.  
For more information, see Making system entitlements requestable on page 189. |
| 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.  
- To specify members of a specific application role as product owners, perform the following under Product owners:  
  1. Enable the Select from roles option.  
  2. In the Product owner field, click Assign/Change.  
  3. In the Edit Product Owner pane, click the |
To specify a specific identity as the product owner, perform the following under **Product owners**:

1. 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 Data Explorer navigation, click **System entitlements**.
3. On the **System Entitlements** page, click the system entitlement whose service item you want to edit.
4. In the **Edit System Entitlement** pane, click the **Details** tab.
5. On the **Service Item** tab, edit the service item's main data.

**Table 28: Main data of system entitlement service items**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service item</td>
<td>Enter a name for the service item.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the service item.</td>
</tr>
<tr>
<td>Service category</td>
<td>You can group different service items into service categories. To do this, click <strong>Assign/Change</strong> 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 41.</td>
</tr>
<tr>
<td>Approval policy</td>
<td>Select the approval policy used to determine the approver when the service item is requested in the Web Portal.</td>
</tr>
<tr>
<td>Max. days valid</td>
<td>Specify how long an identity can keep the product until it is automatically unsubscribed again.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>An identity</td>
<td>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.</td>
</tr>
<tr>
<td>Web page</td>
<td>Specify the URL of a web page that contains more information about the product. Use the following format: <a href="https://www.example.com">https://www.example.com</a> or <a href="http://www.example.com">http://www.example.com</a>. This field allows you to link product descriptions in the internet or intranet to the service item.</td>
</tr>
<tr>
<td>Sort order</td>
<td>Specify how the service category is sorted.</td>
</tr>
<tr>
<td>Request property</td>
<td>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.</td>
</tr>
<tr>
<td>Functional area</td>
<td>Click Assign/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 One Identity Manager Risk Assessment Administration Guide.</td>
</tr>
<tr>
<td>Attestor</td>
<td>Click Assign/Change and then select an application role. Members of this application role can approve attestation cases that affect the service item.</td>
</tr>
<tr>
<td>Terms of use</td>
<td>Select the terms of use that the product's requester must accept.</td>
</tr>
<tr>
<td>Picture</td>
<td>Enter a picture for the service item. Users see this picture when they make a request. Perform the following actions as well:</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Request parameters must be defined per recipient</td>
<td>Select the check box to enter additional request properties separately for each recipient of this product, if the product is requested for different recipients in one request procedure.</td>
</tr>
<tr>
<td>Retain service item assignment on relocation</td>
<td>Select the check box if requests for this service item are 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.</td>
</tr>
<tr>
<td>Tags</td>
<td>Enter tags for the product. These tags can be used as search criteria by requests in the Web Portal.</td>
</tr>
<tr>
<td>Not requestable/Requestable</td>
<td>Set the switch to <strong>Requestable</strong> if you want to request system entitlements through the Web Portal.</td>
</tr>
<tr>
<td></td>
<td>Set the switch to <strong>Not requestable</strong> if you do not want to request system entitlements through the Web Portal.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <strong>Making system entitlements requestable</strong> on page 189.</td>
</tr>
<tr>
<td>Product owner</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• To specify members of a specific application role as product owners, perform the following under <strong>Product owners</strong>:&lt;br&gt;1. Enable the <strong>Select from roles</strong> option.&lt;br&gt;2. In the <strong>Product owner</strong> field, click <strong>Assign/Change</strong>.&lt;br&gt;3. In the <strong>Edit Product Owner</strong> pane, click the appropriate application role.&lt;br&gt;• To specify a specific identity as the product owner, perform the following under <strong>Product owners</strong>:&lt;br&gt;1. Enable the <strong>Select from identities</strong> option.&lt;br&gt;2. In the <strong>Identity</strong> list, select the corresponding identity.</td>
</tr>
</tbody>
</table>
6. Click **Save**.

**Related topics**

- Assigning owners to system entitlements on page 178

**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 199
- Analyzing assignments to system entitlements on page 199
- Assigning identity system entitlements on page 200
- Removing system entitlements from identities on page 201

**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. In the list, 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 system entitlements**

You can see 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. In the **Edit System Entitlement** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Direct memberships** or **Inherited memberships**.
6. Next to the appropriate membership, click **View assignment analysis**.

Assigning identity system entitlements

You can assign system entitlements to identities. You do this through requests.

To assign a system entitlement to 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 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 **Select Identities** pane, select the check box next to the identity you want to assign to the system entitlement.
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.

To re-add an excluded member

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click .
3. In the pane, click the **Memberships** tab.
4. On the **Memberships** tab, click **Excluded members**.
5. Select the check box in front of the identity you want to add again as a member.
6. Click **Remove exclusion**.
Related topics

- Requesting products on page 50

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 Delete.
   - If it is an indirect assignment, click Unsubscribe.
   
     NOTE: You can only unsubscribe memberships that you have requested yourself.
8. In the Delete Memberships or Unsubscribe Memberships dialog, confirm the prompt with OK.

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 entitlement child groups on page 202
Displaying system entitlement child groups

You can see 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.

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 202
- Approving and denying attestation cases of system entitlements on page 203

Displaying attestation cases of system entitlements

You can see 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 Details next to the attestation case.
Approval and denying attestation cases of system entitlements

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

**To approve an attestation case**

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation, click **System entitlements**.
3. In the list, click the system entitlement whose attestation case is 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, select the **Pending** option.
7. Perform one of the following actions:
   - To approve an attestation case, in the list, select the check box next to the attestation case and click **Approve** below the list.
   - To deny an attestation case, in the list, select the check box next to the attestation case and click **Deny** below the list.
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 85
- **Displaying pending attestation cases** on page 104
Creating reports about system entitlements

You can create reports about system entitlement data.

To create a report about a system entitlement
1. In the menu bar click Data administration > Data Explorer.
2. In the Data Explorer 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 Entitlement, click Download report.

Managing departments

You can use the Web Portal to manage departments.

Detailed information about this topic
- Displaying departments on page 204
- Displaying and editing department main data on page 204
- Managing department memberships on page 206
- Managing department entitlements on page 208

Displaying departments

You can see any of the departments and their details.

To display departments
1. In the menu bar click Data administration > Data Explorer.
2. In the Data Explorer navigation click Departments.
   This opens the Departments page and displays all the departments.
3. (Optional) To display details of a department, next to the department, click Edit.

Displaying and editing department main data

You can see 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 Data Explorer navigation, click Departments.
3. On the Departments page, next to the department whose main data you want to display, click Edit.
4. In the Edit Department pane, make your changes in the relevant fields.

Table 29: Department main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Enter a full, descriptive name for the department.</td>
</tr>
<tr>
<td>Short name</td>
<td>Enter a short name for the department.</td>
</tr>
<tr>
<td>Object ID</td>
<td>Enter a unique object ID for the department. For example, the object ID is required in SAP systems for assigning identities to departments.</td>
</tr>
<tr>
<td>Parent department</td>
<td>Click <strong>Assign/Change</strong> 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.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select the manager who is responsible for the department.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>Select an identity to act as a deputy to the department’s manager.</td>
</tr>
<tr>
<td>Additional manager</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role are responsible for the department.</td>
</tr>
<tr>
<td>Location</td>
<td>Click <strong>Assign/Change</strong> and select the location the cost center is primarily assigned to.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role can approve attestation cases for the department.</td>
</tr>
<tr>
<td>Cost center</td>
<td>Click <strong>Assign/Change</strong> and select the location the department is primarily assigned to.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the department.</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the department.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the department.</td>
</tr>
</tbody>
</table>

5. Click Save.
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 206
- Analyzing assignments to departments on page 206
- Adding identities to departments on page 207
- Removing identities from departments on page 208

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. In the list, next to the department whose memberships you want to display, click Edit.
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 see 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, next to the department whose memberships you want to display, click Edit.
4. In the Edit Department pane, click the Memberships tab.
5. On the **Memberships** tab, click **Secondary memberships**.
6. Next to the corresponding membership, select the check box.
7. Click **View assignment analysis**.

### Adding identities to departments

You can add identities to departments. You do this through requests. In addition, you can re-add members who were originally assigned through a dynamic role but were excluded by removing the exclusion.

**To add an identity 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, next to the department you want to add an identity to, click **Edit**.
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 **Select Identities** pane, select the check box next to the identity you want to assign to the department.
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 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, next to the department you want to add again, click **Edit**.
4. In the **Edit Department** pane, click the **Memberships** tab.
5. On the **Memberships** tab, click **Excluded members**.
6. Select the check box in front of the identity you want to add again as a member.
7. Click **Remove exclusion**.
Related topics

- Requesting products on page 50

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, next to the department with a membership you want to delete, click Edit.
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. In the Remove Memberships pane, click Remove memberships.
9. (Optional) If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the Specify Reason for Exclusion dialog, specify why you want to remove the member.
   b. Click Exclude members.

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 209
- Adding entitlements to departments on page 209
- Deleting department entitlements on page 209
Displaying department entitlements

You can see 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. In the list, next to the department whose entitlements you want to display, click Edit.
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. In the list, next to the department to which you want to add a entitlement, click Edit.
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, 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.
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 50

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. In the list, next to the department from which you want to delete an entitlement, click **Edit**.
4. In the **Edit Department** pane, click the **Entitlements** tab.
5. On the **Entitlement** tab, select the check box next to the entitlement you want to delete.
6. Click **Remove**.
7. In the dialog, confirm the prompt with **Yes**.

**Managing locations**

You can use the Web Portal to manage locations.

**Detailed information about this topic**

- Displaying locations on page 210
- Displaying and editing location main data on page 210
- Managing location memberships on page 212
- Managing location entitlements on page 214

**Displaying locations**

You can see any of the locations and their details.

**To display locations**

1. In the menu bar click **Data administration > Data Explorer**.
2. In the Data Explorer navigation click **Locations**.
   This opens the **Locations** page and displays all the locations.
3. (Optional) To display details of a location, next to the location, click **Edit**.

**Displaying and editing location main data**

You can see 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 Data Explorer navigation, click **Locations**.
3. On the **Locations** page, next to the location whose main data you want to display, click **Edit**.
4. In the **Edit Location** pane, make your changes in the relevant fields.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Enter a full, descriptive name for the location.</td>
</tr>
<tr>
<td>Short name</td>
<td>Enter a short name for the location.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter an additional description for the location.</td>
</tr>
<tr>
<td>Parent location</td>
<td>Click <strong>Assign/Change</strong> 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.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select the manager who is responsible for the location.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>Select an identity to act as a deputy to the location's manager.</td>
</tr>
<tr>
<td>Additional manager</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role are responsible for the location.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role can approve attestation cases for the location.</td>
</tr>
<tr>
<td>Department</td>
<td>Click <strong>Assign/Change</strong> and select the department the location is primarily assigned to.</td>
</tr>
<tr>
<td>Cost center</td>
<td>Click <strong>Assign/Change</strong> and select the cost center the location is primarily assigned to.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the location.</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the location.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the location.</td>
</tr>
</tbody>
</table>

5. Click **Save**.
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 212
- Analyzing assignments to locations on page 212
- Adding identities to locations on page 213
- Removing identities from locations on page 214

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. In the list, next to the location whose memberships you want to display, click Edit.
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 see 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, next to the location whose memberships you want to display, click Edit.
4. In the Edit Location pane, click the Memberships tab.
5. On the Memberships tab, click Secondary memberships.
6. Next to the corresponding membership, select the check box.
7. Click View assignment analysis.

Adding identities to locations

You can add identities to locations. You do this through requests.
In addition, you can re-add members who were originally assigned through a dynamic role but were excluded by removing the exclusion.

To add an identity 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, next to the location you want to add an identity to, click Edit.
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 Select Identities pane, select the check box next to the identity you want to assign to the location.
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 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, next to the location you want to add again, click Edit.
4. In the Edit Location pane, click the Memberships tab.
5. On the Memberships tab, click Excluded members.
6. Select the check box in front of the identity you want to add again as a member.
7. Click Remove exclusion.

Related topics

- Requesting products on page 50
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, next to the location with a membership you want to delete, click Edit.
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. In the Remove Memberships pane, click Remove memberships.
9. (Optional) If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the Specify Reason for Exclusion dialog, specify why you want to remove the member.
   b. Click Exclude members.

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 214
- Adding entitlements to locations on page 215
- Deleting entitlements from locations on page 215

Displaying location entitlements

You can see 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. In the list, next to the location whose entitlements you want to display, click Edit.
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. In the list, next to the location to which you want to add a entitlement, click Edit.
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, 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 50

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. In the list, next to the location from which you want to delete an entitlement, click Edit.
4. In the Edit Location pane, click the Entitlements tab.
5. On the Entitlement tab, select the check box next to the entitlement you want to delete.
6. Click Remove.
7. In the dialog, confirm the prompt with Yes.

Managing cost centers

You can use the Web Portal to manage cost centers.

Detailed information about this topic

Displaying cost centers

You can see 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 Data Explorer 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, next to the cost center, click Edit.

Displaying and editing cost center main data

You can see 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 Data Explorer navigation, click Cost centers.
3. On the Cost Centers page, next to the cost center whose main data you want to display, click Edit.
4. In the **Edit Cost Center** pane, make your changes in the relevant fields.

### Table 31: Cost center main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost center</td>
<td>Enter a full, descriptive name for the cost center.</td>
</tr>
<tr>
<td>Short name</td>
<td>Enter a short name for the cost center.</td>
</tr>
<tr>
<td>Parent cost center</td>
<td>Click <strong>Assign/Change</strong> 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.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select the manager who is responsible for the cost center.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>Select an identity to act as a deputy to the cost center's manager.</td>
</tr>
<tr>
<td>Additional manager</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role are responsible for the department.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role can approve attestation cases for the cost center.</td>
</tr>
<tr>
<td>Department</td>
<td>Click <strong>Assign/Change</strong> and select the department that the cost center is primarily assigned to.</td>
</tr>
<tr>
<td>Location</td>
<td>Click <strong>Assign/Change</strong> and select the location the cost center is primarily assigned to.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the cost center.</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the cost center.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the cost center.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

### 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 218
- Analyzing assignments to cost centers on page 218
- Adding identities to cost centers on page 219
- Removing identities from cost centers on page 219

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. In the list, next to the cost center whose memberships you want to display, click Edit.
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 see 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, next to the cost center whose memberships you want to display, click Edit.
4. In the Edit Cost Center pane, click the Memberships tab.
5. On the Memberships tab, click Secondary memberships.
6. Next to the corresponding membership, select the check box.
7. Click View assignment analysis.
Adding identities to cost centers

You can add identities to cost centers. You do this through requests. In addition, you can re-add members who were originally assigned through a dynamic role but were excluded by removing the exclusion.

To add an identity 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, next to the cost center you want to add an identity to, click Edit.
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 Select Identities pane, select the check box next to the identity you want to assign to the cost center.
8. Click Request memberships.
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 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, next to the cost center you want to add again, click Edit.
4. In the Edit Cost Center pane, click the Memberships tab.
5. On the Memberships tab, click Excluded members.
6. Select the check box in front of the identity you want to add again as a member.
7. Click Remove exclusion.

Related topics

- Requesting products on page 50

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, next to the cost center with a membership you want to delete, click Edit.
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. In the Remove Memberships pane, click Remove memberships.
9. (Optional) If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the Specify Reason for Exclusion dialog, specify why you want to remove the member.
   b. Click Exclude members.

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 220
- Adding entitlements to cost centers on page 221
- Deleting cost center entitlements on page 221

Displaying cost center entitlements

You can see 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. In the list, next to the cost center whose entitlements you want to display, click Edit.
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. In the list, next to the cost center to which you want to add an entitlement, click Edit.
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, 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.
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 50

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. In the list, next to the cost center from which you want to delete an entitlement, click Edit.
4. In the Edit Cost Center pane, click the Entitlements tab.
5. On the Entitlement tab, select the check box next to the entitlement you want to delete.
6. Click Remove.
7. In the dialog, confirm the prompt with Yes.
Managing business roles

You can use the Web Portal to manage business roles.

Detailed information about this topic

- Displaying business roles on page 222
- Displaying and editing business role main data on page 222
- Managing business role memberships on page 224
- Managing business role entitlements on page 226

Displaying business roles

You can see 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 Data Explorer navigation click Business roles.
   This opens the Business Roles page and displays all the business roles.
3. (Optional) To view details of a business role, next to the business role, click Edit.

Displaying and editing business role main data

You can see 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 Data Explorer navigation, click Business roles.
3. On the Business Roles page, next to the business role whose main data you want to display, click Edit.
4. In the **Edit Business Roles** pane, make your changes in the relevant fields.

**Table 32: Business role main data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business role</td>
<td>Enter a full, descriptive name for the business role.</td>
</tr>
<tr>
<td>Short name</td>
<td>Enter a short name for the business role.</td>
</tr>
<tr>
<td>Internal name</td>
<td>Enter a company internal name for the business role.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the business role.</td>
</tr>
<tr>
<td>Role class</td>
<td>When you create the business role: Select the role class of the business role.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Parent business role</td>
<td>Click <strong>Assign/Change</strong> 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.</td>
</tr>
<tr>
<td>Role type</td>
<td>Select the role type of the business role.</td>
</tr>
<tr>
<td></td>
<td>Role types are mainly used to regulate approval policy inheritance.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the business role.</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Click <strong>Assign/Change</strong> and select an application role. Members of the selected application role can approve requests for members of the business role.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select the manager who is responsible for the business role.</td>
</tr>
<tr>
<td>2nd Manager</td>
<td>Select an identity to act as a deputy to the business role's manager.</td>
</tr>
<tr>
<td>Additional manager</td>
<td>Click <strong>Assign/Change</strong> and select a cost center. Members of the selected application role are responsible for the department.</td>
</tr>
<tr>
<td>Employees do not inherit</td>
<td>Select this check box if you want to temporarily prevent identities from inheriting this business role.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a comment for the business role.</td>
</tr>
</tbody>
</table>

5. Click **Save**.
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 224
- Analyzing assignments to business roles on page 224
- Assigning identities to business roles on page 225
- Removing business roles from identities on page 226

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. In the list, next to the business role whose memberships you want to display, click Edit.
4. In the Edit Business Roles 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 assign business roles to identities. The business role is then assigned through a request by displaying an assignment analysis for the corresponding membership.

You can see 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, next to the business role whose memberships you want to display, click **Edit**.

4. In the **Edit Business Roles** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Next to the corresponding membership, select the check box.

7. Click **View assignment analysis**.

## Assigning identities to business roles

You can assign business roles to identities. You do this through requests.

In addition, you can re-add members who were originally assigned through a dynamic role but were excluded by removing the exclusion.

### To assign a business role to 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, next to the business role you want to add an identity to, click **Edit**.

4. In the **Edit Business Roles** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Secondary memberships**.

6. Click **Request memberships**.

7. In the **Select Identities** pane, select the check box next to the identity you want to assign to the business role.

8. Click **Request memberships**.

9. Close the **Edit Business Roles** 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 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, next to the business role you want to add again, click **Edit**.

4. In the **Edit Business Role** pane, click the **Memberships** tab.

5. On the **Memberships** tab, click **Excluded members**.
6. Select the check box in front of the identity you want to add again as a member.
7. Click Remove exclusion.

Related topics
- Requesting products on page 50

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, next to the business role with a membership you want to delete, click Edit.
4. In the Edit Business Roles 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. In the Remove Memberships pane, click Remove memberships.
9. (Optional) If the member was assigned through a dynamic role, perform the following actions:
   a. (Optional) In the Specify Reason for Exclusion dialog, specify why you want to remove the member.
   b. Click Exclude members.

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 227
- Adding entitlements to business roles on page 227
- Deleting business role entitlements on page 227
Displaying business role entitlements

You can see 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. In the list, next to the business role whose entitlements you want to display, click Edit.
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. In the list, next to the business role to which you want to add a entitlement, click Edit.
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, 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.
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 50

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. In the list, next to the business role from which you want to delete an entitlement, click Edit.
4. In the Edit Business Role pane, click the Entitlements tab.
5. On the Entitlement tab, select the check box next to the entitlement you want to delete.
6. Click Remove.
7. In the dialog, confirm the prompt with Yes.

Managing system roles

You can use the Web Portal to manage system roles.

Detailed information about this topic

- Displaying system roles on page 228
- Displaying and editing system role main data on page 228
- Managing system role memberships on page 230
- Managing system role entitlements on page 232

Displaying system roles

You can see 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 Data Explorer navigation click System roles.
   
   This opens the System Roles page and displays all the System roles.
3. (Optional) To display details of a system role, click Edit next to the system role.

Displaying and editing system role main data

You can see 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 Data Explorer navigation, click **System roles**.
3. On the **System Roles** page, next to the system role whose main data you want to display, click **Edit**.
4. In the **Edit System Role** pane, make your changes in the relevant fields.

### Table 33: System role main data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System role</td>
<td>Enter a full, descriptive name for the system role.</td>
</tr>
<tr>
<td>Display name</td>
<td>Enter a name for displaying the system role in the One Identity Manager tools.</td>
</tr>
<tr>
<td>Internal product name</td>
<td>Enter a company internal name for the system role.</td>
</tr>
<tr>
<td>System role type</td>
<td>Select the role type of the system role.</td>
</tr>
<tr>
<td></td>
<td>The system role type specifies which type of company resources make up the system role.</td>
</tr>
<tr>
<td>Service item</td>
<td>Shows you the associated service item.</td>
</tr>
<tr>
<td>System role manager</td>
<td>Click <strong>Change</strong> and select the identity responsible for the system role.</td>
</tr>
<tr>
<td></td>
<td>This identity can edit the system role's main data and be used as an attester for system role properties.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Comment</td>
<td>Enter a comment for the system role.</td>
</tr>
<tr>
<td>IT shop</td>
<td>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 the request granted by a defined approval process. The system role can still be assigned directly to identities and hierarchical roles. For detailed information about IT Shop, see the <em>One Identity Manager IT Shop Administration Guide</em>.</td>
</tr>
<tr>
<td>Only use in IT Shop</td>
<td>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 the request granted by a defined approval process. The system role may not be assigned directly to hierarchical roles.</td>
</tr>
</tbody>
</table>

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 230
- Analyzing assignments to system roles on page 230
- Assigning identities to system roles on page 231
- Removing identities from my system roles on page 231

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. In the list, next to the system role whose memberships you want to display, click Edit.
4. In the Edit System Role pane, click the Memberships tab.

Analyzing assignments to system roles

You can see 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, next to the system role whose memberships you want to display, click Edit.
4. In the Edit System Role pane, click the Memberships tab.
5. On the Memberships tab, select the check box next to the corresponding membership.
6. Click View assignment analysis.
Assigning identities to system roles

You can assign system roles to identities. You do this through requests.

To assign a system role to 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, next to the system role you want to add an identity to, click Edit.
4. In the Edit System Role pane, click the Memberships tab.
5. On the Memberships tab, click Request memberships.
6. In the Select Identities pane, select the check box next to the identity you want to assign to the system role.
7. Click Request memberships.
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.

To re-add an excluded member

1. In the menu bar click Data administration > Data Explorer.
2. In the Data Explorer navigation, click .
3. In the pane, click the Memberships tab.
4. On the Memberships tab, click Excluded members.
5. Select the check box in front of the identity you want to add again as a member.
6. Click Remove exclusion.

Related topics

- Requesting products on page 50

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, next to the system role with a membership you want to delete, click Edit.
4. In the Edit System 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. In the Remove Memberships pane, click Remove memberships.

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 232
- Adding entitlements to system roles on page 232
- Deleting system role entitlements on page 233

Displaying system role entitlements

You can see 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. In the list, next to the system role whose entitlements you want to display, click Edit.
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. In the list, next to the system role to which you want to add a entitlement, click Edit.
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, 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.
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 50

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. In the list, next to the system role from which you want to delete an entitlement, click Edit.
4. In the Edit System Role pane, click the Entitlements tab.
5. On the Entitlement tab, select the check box next to the entitlement you want to delete.
6. Click Remove.
7. In the 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 88 or Editing attestation policies on page 90), 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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All departments</td>
<td>Attests primary memberships in all departments.</td>
</tr>
<tr>
<td>Specific departments</td>
<td>Select the departments with primary memberships to attest. Use <code>enter</code> and <code>esc</code> to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific child departments</td>
<td>Select the departments with primary memberships to attest. In addition, primary memberships of all child departments under this</td>
</tr>
</tbody>
</table>

One Identity Manager On Demand Web Portal User Guide
Appendix: Attestation conditions and approval policies from attestation procedures
<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>department are attested.</td>
<td>Use上下和左右 to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Departments with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attest primary memberships in departments with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Departments with matching name</td>
<td>Enter part of a name of departments with primary memberships to attest. All departments that have this pattern in their name are included. Example: <em>Per</em> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

## Attesting primary business roles

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All business roles</td>
<td>Attests primary memberships in all business roles.</td>
</tr>
<tr>
<td>Specific business roles</td>
<td>Select the business roles with primary memberships to attest. Use上下和左右 to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific child business roles</td>
<td>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上下和左右 to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Business roles with specific role classes</td>
<td>Select the role classes. Attests primary membership in business roles with this role class.</td>
</tr>
<tr>
<td>Business roles with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attest primary memberships in business roles with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Business roles with matching name</td>
<td>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: <em>Per</em> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>
# Attesting primary cost centers

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All cost centers</td>
<td>Attests primary memberships in all cost centers.</td>
</tr>
<tr>
<td>Specific cost centers</td>
<td>Select the cost centers with primary memberships to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific child cost centers</td>
<td>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.</td>
</tr>
<tr>
<td>Cost centers with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests primary memberships in cost centers with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Cost centers with matching name</td>
<td>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: <em>Per</em> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

# Attesting primary locations

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All locations</td>
<td>Attests primary memberships in all locations.</td>
</tr>
<tr>
<td>Specific locations</td>
<td>Select the locations with primary memberships to attest. Use  and  to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific child locations</td>
<td>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.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Locations with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests primary memberships in locations with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Locations with matching name</td>
<td>Enter part of a name of locations with primary memberships to attest. All locations that have this pattern in their name are included. Example: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

**Attesting secondary departments**

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All departments</td>
<td>Attests secondary memberships in all departments.</td>
</tr>
<tr>
<td>Specific departments</td>
<td>Select the departments with secondary memberships to attest. Use ☐ and ☒ to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific child departments</td>
<td>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.</td>
</tr>
<tr>
<td>Departments with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests secondary memberships in departments with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Departments with matching name</td>
<td>Enter part of a name of departments with secondary memberships to attest. All departments that have this pattern in their name are included. Example: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>
Attesting secondary cost centers

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All cost centers</td>
<td>Attests secondary memberships in all cost centers.</td>
</tr>
<tr>
<td>Specific cost centers</td>
<td>Select the cost centers with secondary memberships to attest. Use ⌈ and ⌊ to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific child cost centers</td>
<td>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.</td>
</tr>
<tr>
<td>Cost centers with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests secondary memberships in cost centers with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Cost centers with matching name</td>
<td>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: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

Attesting secondary locations

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All locations</td>
<td>Attests secondary memberships in all locations.</td>
</tr>
<tr>
<td>Specific locations</td>
<td>Select the locations with secondary memberships to attest. Use ⌈ and ⌊ to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific child locations</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Attesting PAM asset groups**

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All PAM asset groups</td>
<td>Attests all PAM assets groups.</td>
</tr>
<tr>
<td>Specific PAM asset groups</td>
<td>Select the PAM asset groups to attest.</td>
</tr>
<tr>
<td>PAM asset groups on specific systems</td>
<td>Select the PAM appliances with PAM asset groups to attest.</td>
</tr>
<tr>
<td>PAM asset groups with matching name</td>
<td>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: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

**Attesting PAM asset accounts**

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All PAM asset accounts</td>
<td>Attests all PAM asset accounts.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Specific PAN asset accounts</td>
<td>Select the PAM asset accounts to attest.</td>
</tr>
<tr>
<td>PAM asset accounts on specific systems</td>
<td>Select the PAM appliances with PAM asset accounts to attest.</td>
</tr>
<tr>
<td>PAM asset accounts with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

**Attesting PAM assets**

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All PAM assets</td>
<td>Attests all PAM assets.</td>
</tr>
<tr>
<td>Specific PAM assets</td>
<td>Select the PAM assets to attest.</td>
</tr>
<tr>
<td>PAM assets on specific systems</td>
<td>Select the PAM appliances with PAM asset to attest.</td>
</tr>
<tr>
<td>PAM assets with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

**Attesting PAM user groups**

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All PAM user groups</td>
<td>Attests all PAM user groups.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Specific PAM user groups</td>
<td>Select the PAM user groups to attest.</td>
</tr>
<tr>
<td>PAM user groups with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

### Attesting PAM user accounts

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All PAM user accounts</td>
<td>Attests all PAM user accounts.</td>
</tr>
<tr>
<td>Specific permissions</td>
<td>Select the permissions. Attests PAM user accounts with these permissions.</td>
</tr>
<tr>
<td>Specific PAM user accounts</td>
<td>Select the PAM user accounts to attest.</td>
</tr>
<tr>
<td>PAM user accounts in specific user groups</td>
<td>Select the user groups. Attests PAM user accounts that belong to these user groups.</td>
</tr>
<tr>
<td>PAM user groups on specific systems</td>
<td>Select the PAM appliances with PAM user groups to attest.</td>
</tr>
<tr>
<td>PAM user accounts mapped to specific employees</td>
<td>Select the identities. Attests PAM user accounts that are assigned these identities.</td>
</tr>
<tr>
<td>PAM user accounts with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>
Attesting PAM account groups

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All PAM account groups</td>
<td>Attests all PAM account groups.</td>
</tr>
<tr>
<td>Specific PAM account groups</td>
<td>Select the PAM account groups to attest.</td>
</tr>
<tr>
<td>PAM user accounts on specific systems</td>
<td>Select the PAM appliances with PAM user accounts to attest.</td>
</tr>
<tr>
<td>PAM account groups on specific systems</td>
<td>Select the PAM appliances with PAM account groups to attest.</td>
</tr>
<tr>
<td>PAM account groups with matching name</td>
<td>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: <em>Per</em> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

Attesting PAM directory accounts

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All PAM directory accounts</td>
<td>Attests all PAM directory accounts.</td>
</tr>
<tr>
<td>Specific PAM directory accounts</td>
<td>Select the PAM directory accounts to attest.</td>
</tr>
<tr>
<td>PAM directory accounts on specific directories</td>
<td>Select the directories. Attests directory accounts that are found in this directory.</td>
</tr>
</tbody>
</table>
Attesting PAM accesses

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All PAM accesses</td>
<td>Attests all PAM access.</td>
</tr>
<tr>
<td>Specific PAM asset accounts</td>
<td>Select the PAM asset accounts with access to attest.</td>
</tr>
<tr>
<td>Specific PAM assets</td>
<td>Select the PAM assets with access to attest.</td>
</tr>
<tr>
<td>Specific PAM user accounts</td>
<td>Select the PAM user accounts with access to attest.</td>
</tr>
<tr>
<td>Specific PAM directory accounts</td>
<td>Select the PAM directory accounts with access to attest.</td>
</tr>
<tr>
<td>Specific PAM directories</td>
<td>Select PAM directories. Attests access to these PAM directories.</td>
</tr>
<tr>
<td>Specific access type</td>
<td>Select access types. Attests access that uses one of these access types.</td>
</tr>
<tr>
<td>PAM user accounts mapped to specific employees</td>
<td>Select the identities. Attests access through PAM user accounts with these identities assigned to them.</td>
</tr>
<tr>
<td>PAM user accounts with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests access through PAM user accounts with a risk index in the chosen range.</td>
</tr>
</tbody>
</table>
| PAM user | Enter part of a name of PAM user accounts with access to attest. All PAM
### Condition | Description
---|---
Accounts with matching name | User accounts that have this pattern in their name are included. Example: **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:

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

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

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

### 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:
### 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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All business roles</td>
<td>Attests all business roles.</td>
</tr>
<tr>
<td>Specific business roles</td>
<td>Select the business roles to attest. Use ↑ and ↓ to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Business roles with specific role classes</td>
<td>Select the role classes. Attests business roles with these role classes.</td>
</tr>
<tr>
<td>Business roles with defined risk index</td>
<td>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.</td>
</tr>
</tbody>
</table>

---

### Approval policies

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

<table>
<thead>
<tr>
<th>Approval policies</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation by selected approvers</td>
<td>Click Assign/Change in the Attestors field and then select the identities that can make approval decisions about attestation cases.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Business roles with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

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

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

**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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All cost centers</td>
<td>Attests all cost centers.</td>
</tr>
<tr>
<td>Specific cost centers</td>
<td>Select the cost centers to attest. Use and to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Cost centers with defined risk index</td>
<td>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.</td>
</tr>
<tr>
<td>Cost centers with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

For this attestation procedure, you can use the following attestation policies:
Attestation of locations by manager

- Location 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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All locations</td>
<td>Attests all locations.</td>
</tr>
<tr>
<td>Specific locations</td>
<td>Select the locations to attest. Use ( \Rightarrow ) and ( \Leftarrow ) to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Locations with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests locations with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Locations with matching name</td>
<td>Enter part of a name of locations with access to attest. All locations that have this pattern in their name are included. Example: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All system roles</td>
<td>Attests all system roles.</td>
</tr>
<tr>
<td>Specific system roles</td>
<td>Select the system roles to attest. Use ▲ and ▼ to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>System roles by applications</td>
<td>Select the applications (Application Governance). Attests system roles that are assigned to these applications.</td>
</tr>
<tr>
<td>System roles with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests system roles with a risk index in the chosen range.</td>
</tr>
<tr>
<td>System roles with matching name</td>
<td>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: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

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

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

**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:
<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All system entitlements</td>
<td>Attests memberships in all system entitlements.</td>
</tr>
<tr>
<td>Specific employees</td>
<td>Select the identities. Attests this identity's memberships (or their associated user accounts) in system entitlements.</td>
</tr>
<tr>
<td>Specific employees with subidentities.</td>
<td>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.</td>
</tr>
<tr>
<td>Specific system entitlements</td>
<td>Select the system entitlements. Attests memberships in these system entitlements.</td>
</tr>
</tbody>
</table>
| Membership by attestation state | Select an attestation status. Attests memberships in system entitlements that match this attestation status.  
  - **Denied memberships**: Attests memberships that have been denied.  
  - **All Memberships**: Attests all memberships.  
  - **New memberships**: Attests memberships that have never been attested. |
<p>| New or not attested for x days | Specify a number of days. Attests memberships in system entitlements that have not been attested for the defined number of days. |
| No dynamic groups from Active Roles | Attests memberships in all system entitlements. Dynamic groups are ignored in the process. |
| System entitlements with specific owners | Select the identities. Attests memberships in system entitlements that are managed by these identities. |
| System entitlements in a target system container | Select the target system containers. Attests memberships in system entitlements found in these target system containers. |
| System entitlements in target systems | Select the target systems. Attests memberships in system entitlements assigned to these target systems. |
| System entitlements with defined | Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests memberships in system entitlements with a risk index in the chosen range. |</p>
<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>risk index</td>
<td>Select the departments. Attests memberships in system entitlements that are managed by the identities in these departments.</td>
</tr>
<tr>
<td>System entitlements with owners in departments</td>
<td>Attests user account memberships in system entitlements that only have one owner.</td>
</tr>
<tr>
<td>System entitlements with any owner</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>System entitlements by applications</td>
<td>Select the applications. Attests user account memberships in system entitlements that are assigned to these applications.</td>
</tr>
<tr>
<td>System entitlements by assignment origin</td>
<td>Select how user account memberships in system entitlements must be assigned to enable attestation:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Directly assigned</strong>: Attests memberships that were assigned directly.</td>
</tr>
<tr>
<td></td>
<td>- <strong>By request</strong>: Attests memberships in system entitlements that were requested.</td>
</tr>
<tr>
<td></td>
<td>- <strong>By dynamic roles</strong>: Attests memberships in system entitlements that were assigned through dynamic roles.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Through roles</strong>: Attests memberships in system entitlements that were assigned through roles.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Through system roles</strong>: Attests memberships in system entitlements that were assigned through system roles.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Approval policies</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation by selected approvers</td>
<td>Click Assign/Change in the Attestors field and then select the identities that can make approval decisions about attestation cases.</td>
</tr>
<tr>
<td>Attestation by selected approvers with automatic removal of assignments</td>
<td>Click Assign/Change in the Attestors field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied</td>
</tr>
<tr>
<td>Approval policies</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Attestation by entitlement owner with automatic removal of assignments</td>
<td>Product owners of system entitlements can be approved through attestation cases. Memberships are deleted if attestation is denied and the configuration fits.</td>
</tr>
</tbody>
</table>
| Attestation by employee manager and product owner (with peer group analysis) | The following identities can be approved through attestation cases:  
  - Identity managers who are assigned the system entitlements  
  - Product owners of system entitlements after a peer group analysis (see Attestation by peer group analysis on page 101) |
| 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:

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

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

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

### 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:
<table>
<thead>
<tr>
<th><strong>Condition</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>All roles</td>
<td>Attests memberships in all business roles.</td>
</tr>
<tr>
<td>Business roles with matching name</td>
<td>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: <em>Per</em> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>Attesting by attestation status</td>
<td>Select an attestation status Attests memberships in business roles that match this attestation status. You can select the follow status:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Denied memberships</strong>: Attests memberships that have been denied.</td>
</tr>
<tr>
<td></td>
<td>- <strong>All Memberships</strong>: Attests all memberships.</td>
</tr>
<tr>
<td></td>
<td>- <strong>New memberships</strong>: Attests memberships that have never been attested.</td>
</tr>
<tr>
<td>Specific employees</td>
<td>Select the identities. Attests identity memberships in business roles.</td>
</tr>
<tr>
<td>Specific employees with subidentities.</td>
<td>Select the identities. Attests identity memberships in business roles. In addition, this identity’s subidentities memberships in business roles are attested.</td>
</tr>
<tr>
<td>Specific roles</td>
<td>Select the business roles. Attests memberships in these business roles. Use ⌂ and ⌊ to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Specify a number of days. Attests memberships in business roles that have not been attested for the defined number of days.</td>
</tr>
<tr>
<td>Roles with specific owners</td>
<td>Select the identities. Attests memberships in business roles of identities who are owners of these business roles.</td>
</tr>
<tr>
<td>Roles with specific role classes</td>
<td>Select the role classes. Attests membership in business roles of this role class.</td>
</tr>
<tr>
<td>Roles with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests memberships in business roles with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Roles with any owner</td>
<td>Attests all memberships in business roles that have an owner.</td>
</tr>
<tr>
<td>Roles with owners in departments</td>
<td>Select the departments. Attests all business roles that have an owner in the selected department.</td>
</tr>
</tbody>
</table>
### Roles by assignment type

Select how memberships in business roles must be assigned to enable attestation:

- **Directly assigned**: Attests memberships that were assigned directly.
- **By request**: Attests memberships that were requested.
- **By delegation**: Attests memberships that were delegated.
- **By dynamic role**: Attests memberships that were attested through dynamic roles.

### Approval policies

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

### Attesting 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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All roles</td>
<td>Attests memberships in all system roles.</td>
</tr>
<tr>
<td>System roles with matching name</td>
<td>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: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>
| Attesting by attestation status | Select an attestation status. Attests memberships in system roles that match this attestation status. You can select the follow status:  
  
  - **Denied memberships**: Attests memberships that have been denied.  
  - **All Memberships**: Attests all memberships. |
**Condition** | **Description**
--- | ---
- **New memberships**: Attests memberships that have never been attested.

**Specific roles**
Select the system roles. Attests memberships in these system roles. Use \[ \text{ ]} \] and \[ \text{ ]} \] to switch between hierarchical and list view. Multi-select is possible.

**New or not attested for x days**
Specify a number of days. Attests memberships in system roles that have not been attested for the defined number of days.

**Roles with specific owners**
Select the identities. Attests memberships in system roles of identities who are owners of these system roles.

**Roles with defined risk index**
Use the **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:
- **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**
Click **Assign/Change** in the **Attestors** field and then select the identities that can make approval decisions about attestation cases. Memberships are deleted if attestation is denied and the configuration fits.
Attesting device owners

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All devices</td>
<td>Attests owners of all the devices.</td>
</tr>
</tbody>
</table>

Attesting system entitlement owners

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All system entitlements</td>
<td>Attests owners of all system entitlements.</td>
</tr>
<tr>
<td>System entitlements by applications</td>
<td>Select the applications. Attests system entitlements owners to which the applications are assigned.</td>
</tr>
</tbody>
</table>

Attesting system entitlement owners (initial)

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

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All system entitlements without owner</td>
<td>Attests initial assignments of owners to system entitlements that do not have product owners.</td>
</tr>
<tr>
<td>No dynamic groups from Active Roles</td>
<td>Attests initial assignment of product owners to system entitlements. Dynamic groups are ignored in the process.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation of ownership by proposed new owner</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All user accounts</td>
<td>Attests all user accounts.</td>
</tr>
<tr>
<td>All privileged user accounts</td>
<td>Attests all privileged user accounts.</td>
</tr>
<tr>
<td>User accounts in the target system</td>
<td>Select the target systems. Attests user accounts assigned to these target systems.</td>
</tr>
<tr>
<td>User accounts of specific employees</td>
<td>Select the identities. Attests user accounts assigned to these identities.</td>
</tr>
<tr>
<td>Specific user accounts</td>
<td>Select the user accounts to attest. Use 📈 and 📝 to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>User accounts with defined risk index</td>
<td>Specify a risk index range. Attests user accounts with a risk index in the chosen range.</td>
</tr>
<tr>
<td>User accounts with matching name</td>
<td>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: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>User accounts with employees in departments</td>
<td>Select the departments. Attests user accounts with identities assigned to these departments. Use 📈 and 📝 to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>User accounts of employees in child departments</td>
<td>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.</td>
</tr>
<tr>
<td>User accounts of employees with matching names</td>
<td>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: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>New or not</td>
<td>Specify a number of days. Attests user accounts that have not been...</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>attested for x days</td>
<td>attested for the defined number of days.</td>
</tr>
<tr>
<td>All user accounts not assigned to an identity</td>
<td>Only attests user accounts not assigned to an identity (so-called orphaned user accounts).</td>
</tr>
<tr>
<td>Linked user accounts</td>
<td>Attests only user accounts that are assigned these identities.</td>
</tr>
<tr>
<td>Target system type</td>
<td>Select the target systems types. Attests user accounts in target system of this target system type.</td>
</tr>
</tbody>
</table>

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

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

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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All system entitlements</td>
<td>Attests all system entitlements.</td>
</tr>
<tr>
<td>Specific system entitlements</td>
<td>Select the system entitlements to attest. Use 🔖 and 📝 to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>No dynamic groups from Active Roles</td>
<td>Attests all system entitlements. Dynamic groups are ignored in the process.</td>
</tr>
<tr>
<td>System entitlements with defined risk index</td>
<td>Specify a risk index range. Attests system entitlements with a risk index in the chosen range.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Approval policies</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attestation of system entitlements by product owner (OA)</td>
<td>Product owners of system entitlements can be approved through attestation cases.</td>
</tr>
<tr>
<td>Attestation by target system manager</td>
<td>Target system managers can be approved through attestation cases.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All departments</td>
<td>Attests assignments of system entitlements to all departments.</td>
</tr>
<tr>
<td>All system entitlements</td>
<td>Attests assignments of all system entitlements to departments.</td>
</tr>
</tbody>
</table>
| Attesting by attestation status | Select an attestation status Attests assignments of system entitlements, matching this attestation status, to departments. You can select the follow status:

  - **Denied memberships**: Attests assignments that have been denied.
  - **All Memberships**: Attests all assignments.
  - **New memberships**: Attests assignments that have never been attested.

| Specific | Select the departments with system entitlements to attest. |
### 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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All business roles</td>
<td>Attests assignments of system entitlements to all business roles.</td>
</tr>
<tr>
<td>All system entitlements</td>
<td>Attests assignments of all system entitlements to business roles.</td>
</tr>
<tr>
<td>Attesting by attestation</td>
<td>Select an attestation status. Attests assignments of system entitlements, matching this attestation status, to business roles.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>status</td>
<td>You can select the follow status:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Denied memberships</strong>: Attests assignments that have been denied.</td>
</tr>
<tr>
<td></td>
<td>- <strong>All Memberships</strong>: Attests all assignments.</td>
</tr>
<tr>
<td></td>
<td>- <strong>New memberships</strong>: Attests assignments that have never been attested.</td>
</tr>
<tr>
<td>Specific business roles</td>
<td>Select the business roles with system entitlements to attest.</td>
</tr>
<tr>
<td></td>
<td>Use  and  to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific system entitlements</td>
<td>Select the with system entitlements with assignments to business roles to attest.</td>
</tr>
<tr>
<td>Business roles with specific role classes</td>
<td>Select the role classes. Attests system entitlement assignments to business roles with these role classes.</td>
</tr>
<tr>
<td>Business roles with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests system entitlement assignments to business roles with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Business roles with matching name</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Example: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Specify a number of days. Attests system entitlement assignments to business roles that have not been attested for the defined number of days.</td>
</tr>
<tr>
<td>System entitlements with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to business roles.</td>
</tr>
<tr>
<td>System entitlements with matching name</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Example: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All cost centers</td>
<td>Attests assignments of system entitlements to all cost centers.</td>
</tr>
<tr>
<td>All system entitlements</td>
<td>Attests assignments of all system entitlements to cost centers.</td>
</tr>
<tr>
<td>Attesting by attestation status</td>
<td>Select an attestation status Attests assignments of system entitlements, matching this attestation status, to cost centers. You can select the follow status:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Denied memberships</strong>: Attests assignments that have been denied.</td>
</tr>
<tr>
<td></td>
<td>• <strong>All Memberships</strong>: Attests all assignments.</td>
</tr>
<tr>
<td></td>
<td>• <strong>New memberships</strong>: Attests assignments that have never been attested.</td>
</tr>
<tr>
<td>Specific cost centers</td>
<td>Select the cost centers with system entitlements to attest. Use ☰ and ☰ to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific system entitlements</td>
<td>Select the with system entitlements with assignments to cost centers to attest.</td>
</tr>
<tr>
<td>Cost centers with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests system entitlement assignments to cost centers with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Cost centers with matching name</td>
<td>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: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Specify a number of days. Attests system entitlement assignments to cost centers that have not been attested for the defined number of days.</td>
</tr>
<tr>
<td>System entitlements with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests assignments of system entitlements, with a risk index in the chosen range, to cost centers.</td>
</tr>
</tbody>
</table>
### Condition | Description
--- | ---
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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All locations</td>
<td>Attests assignments of system entitlements to all locations.</td>
</tr>
<tr>
<td>All system entitlements</td>
<td>Attests assignments of all system entitlements to locations.</td>
</tr>
<tr>
<td>Attesting by attestation status</td>
<td>Select an attestation status Attests assignments of system entitlements, matching this attestation status, to locations. You can select the follow status:</td>
</tr>
<tr>
<td></td>
<td><strong>Denied memberships</strong>: Attests assignments that have been denied.</td>
</tr>
<tr>
<td></td>
<td><strong>All Memberships</strong>: Attests all assignments.</td>
</tr>
<tr>
<td></td>
<td><strong>New memberships</strong>: Attests assignments that have never been attested.</td>
</tr>
<tr>
<td>Specific locations</td>
<td>Select the locations with system entitlements to attest. Use 🔌 and 🔍 to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific system entitlements</td>
<td>Select the with system entitlements with assignments to locations to attest.</td>
</tr>
<tr>
<td>Locations with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests system entitlement assignments to locations with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Locations with matching name</td>
<td>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: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Specify a number of days. Attests system entitlement assignments to locations that have not been attested for the defined number of days.</td>
</tr>
<tr>
<td>System entitlements with defined risk index</td>
<td>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.</td>
</tr>
<tr>
<td>System entitlements with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All departments</td>
<td>Assignments of system roles to all departments</td>
</tr>
<tr>
<td>All system roles</td>
<td>Attests assignments of all system roles to departments.</td>
</tr>
<tr>
<td>Attesting by attestation status</td>
<td>Select an attestation status Attests assignments of system roles, matching this attestation status, to departments. You can select the follow status:</td>
</tr>
<tr>
<td></td>
<td>• Denied memberships: Attests assignments that have been denied.</td>
</tr>
<tr>
<td></td>
<td>• All Memberships: Attests all assignments.</td>
</tr>
<tr>
<td></td>
<td>• New memberships: Attests assignments that have never been attested.</td>
</tr>
<tr>
<td>Specific departments</td>
<td>Select the departments with system roles to attest. Use ‑ and ‑ to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific</td>
<td>Select the with system roles with assignments to departments to attest.</td>
</tr>
</tbody>
</table>
### Condition Description

| System roles | 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 defined risk index | 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. |
| Departments with matching name | Specify a number of days. Attests system role assignments to departments that have not been attested for the defined number of days. |
| New or not attested for x days | 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 defined risk index | 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. |
| System roles with matching name | **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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All business roles</td>
<td>Attests assignments of system roles to all business roles.</td>
</tr>
<tr>
<td>All system roles</td>
<td>Attests assignments of all system roles to business roles.</td>
</tr>
<tr>
<td>Attesting by attestation status</td>
<td>Select an attestation status Attests assignments of system roles, matching this attestation status, to business roles. You can select the follow status:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Denied memberships</strong>: Attests assignments that have been denied.</td>
</tr>
<tr>
<td></td>
<td>- <strong>All Memberships</strong>: Attests all assignments.</td>
</tr>
<tr>
<td></td>
<td>- <strong>New memberships</strong>: Attests assignments that have never been attested.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Specific business roles</td>
<td>Select the business roles with system roles to attest. Use ( \text{△} ) and ( \text{□} ) to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific system roles</td>
<td>Select the business roles with system roles to attest.</td>
</tr>
<tr>
<td>Business roles with specific role classes</td>
<td>Select the role classes. Attests system roles assignments to business roles with these role classes.</td>
</tr>
<tr>
<td>Business roles with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests system roles assignments to business roles with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Business roles with matching name</td>
<td>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: <em>Per</em> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Specify a number of days. Attests system role assignments to business roles that have not been attested for the defined number of days.</td>
</tr>
<tr>
<td>System roles with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to business roles.</td>
</tr>
<tr>
<td>System roles with matching name</td>
<td>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: <em>Per</em> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All cost centers</td>
<td>Attest assignments of system roles to all cost centers.</td>
</tr>
<tr>
<td>All system</td>
<td>Attest assignments of all system roles to cost centers.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>roles</td>
<td>Select an attestation status Attests assignments of system roles, matching this attestation status, to cost centers. You can select the follow status:</td>
</tr>
<tr>
<td></td>
<td>• Denied memberships: Attests assignments that have been denied.</td>
</tr>
<tr>
<td></td>
<td>• All Memberships: Attests all assignments.</td>
</tr>
<tr>
<td></td>
<td>• New memberships: Attests assignments that have never been attested.</td>
</tr>
<tr>
<td>Specific cost centers</td>
<td>Select the cost centers with system roles to attest. Use ‹ and › to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific system roles</td>
<td>Select the with system roles with assignments to cost centers to attest.</td>
</tr>
<tr>
<td>Cost centers with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests system role assignments to cost centers with a risk index in the chosen range.</td>
</tr>
<tr>
<td>Cost centers with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Specify a number of days. Attests system role assignments to cost centers that have not been attested for the defined number of days.</td>
</tr>
<tr>
<td>System roles with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to cost centers.</td>
</tr>
<tr>
<td>System roles with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

### 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.
<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All locations</td>
<td>Attests assignments of system roles to all locations.</td>
</tr>
<tr>
<td>All system roles</td>
<td>Attests assignments of all system roles to locations.</td>
</tr>
<tr>
<td>Attesting by attestation status</td>
<td>Select an attestation status Attests assignments of system roles, matching this attestation status, to locations. You can select the follow status:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Denied memberships</strong>: Attests assignments that have been denied.</td>
</tr>
<tr>
<td></td>
<td>- <strong>All Memberships</strong>: Attests all assignments.</td>
</tr>
<tr>
<td></td>
<td>- <strong>New memberships</strong>: Attests assignments that have never been attested.</td>
</tr>
<tr>
<td>Specific locations</td>
<td>Select the locations with system roles to attest. Use ⌐ and ⌐ to switch between hierarchical and list view. Multi-select is possible.</td>
</tr>
<tr>
<td>Specific system roles</td>
<td>Select the with system roles with assignments to locations to attest.</td>
</tr>
<tr>
<td>Locations with defined risk</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests system role assignments to locations with a risk index in the chosen range.</td>
</tr>
<tr>
<td>index</td>
<td></td>
</tr>
<tr>
<td>Locations with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Specify a number of days. Attests system role assignments to locations that have not been attested for the defined number of days.</td>
</tr>
<tr>
<td>System roles with defined risk</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests assignments of system roles, with a risk index in the chosen range, to locations.</td>
</tr>
<tr>
<td>index</td>
<td></td>
</tr>
<tr>
<td>System roles with matching name</td>
<td>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 &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>

**Attesting assignments to system roles**

Assignments to system roles are attested using the **System role membership attestation** attestation procedure.
<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All system roles</td>
<td>Attests assignments to all system roles.</td>
</tr>
<tr>
<td>Attesting by attestation status</td>
<td>Select an attestation status Attests assignments to system roles, matching this attestation status. You can select the follow status:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Denied memberships</strong>: Attests assignments that have been denied.</td>
</tr>
<tr>
<td></td>
<td>- <strong>All Memberships</strong>: Attests all assignments.</td>
</tr>
<tr>
<td></td>
<td>- <strong>New memberships</strong>: Attests assignments that have never been attested.</td>
</tr>
<tr>
<td>Specific system roles</td>
<td>Select the with system roles with assignments to attest.</td>
</tr>
<tr>
<td>New or not attested for x days</td>
<td>Specify a number of days. Attests assignments to system roles that have not been attested for the defined number of days.</td>
</tr>
<tr>
<td>System roles by applications</td>
<td>Select the applications. Attests assignments to system roles assigned to these applications.</td>
</tr>
<tr>
<td>System roles with defined risk index</td>
<td>Use the <strong>Lower limit</strong> and <strong>Upper limit</strong> fields to define a risk index range. Attests assignments to system roles with a risk index in the chosen range.</td>
</tr>
<tr>
<td>System roles with matching name</td>
<td>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: <strong>Per</strong> finds &quot;Person&quot;, &quot;Personal&quot;, &quot;Perfection&quot; and so on.</td>
</tr>
</tbody>
</table>
About us

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

Contacting us

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

Technical support resources

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

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

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

A
add product to cart  50
address book
display  20
application roles  123
approval decision
display  83
approval history
display  83
approve
pending request  70
attestation
by peer group  101
carry out  85
managing attestation policies  86
sample  101
viewing completed attestations  113
attestation sample  101

create
service category  42
cross-functional product  101

D
data
manage  180
date format  24
deactivate
email notification  24
delete
service category  46
shopping cart  57
deny
pending request  70
display
approval decision  83
approval history  83
pending request  69
requestable product  40
service category  42
shopping cart  53

eedit
service category  44
shelf details  37
e-mail notification
deactivate  24
enable  24
enable
  email notification 24

G
  give reason 55
  grant approval
    pending request 70

H
  header 28

I
  identity
    add 135
    edit 135
    manage 180
  identity as request template 59
  interest group 60

J
  button 30-33
  district 33-34

L
  language
    change 24
  log in 14
    Password Reset Portal 15
  log out 14, 16
  login 14

M
  manage
    data 180
    identity 180
    requestable product access 38
    service category 41
  shopping cart 52
  subscription 25
  system entitlements 188
  user accounts 187
  menu bar 29
  My Responsibilities
    manage 116

N
  navigate 16
  number format 24

O
  organization structure
    manage 117
  other identities' products 60

P
  PAG 60
  PAM 60
  password 20, 22
    change 22
  password question 20
    change 20
    create 20
    delete 20
    edit 20
    manage 20
    specify 20
    unlock 20
  Password Reset Portal
    log in 15
  peer group 59-60
peer group analysis
for attestation 101
pending request
approve 70
deny 70
display 69
grant approval 70
privileged access 60
product
add to shelf 40
cross-functional 101
remove from shelf 41
other identities' products 59
edit pending request 69
extend 80
failed 56
invalid 56
manage 30
request group 62
revoke 81
responsibility
application roles 123
rule and policy violation
view reports about rule and policy violation 114

R
reference user 59
request 50, 52, 57
privileged access 60
submit 57
request for multiple identities 56
request function
configure 31
set up 31
request history
display 79
request product 50, 52, 57
from other identities 59
peer group 60
requestable product
display 40
requestable product access
manage 38
requests
act 50
about a reference user 59
for other recipient 58

S
sample data 101
save for later 66
saved for later 66-69
serve 16
service category
create 42
delete 46
display 42
edit 44
manage 41
set validity period 54
setup
request function 31
shelf
add product 40
clean up products 41
shelf details
edit 37
shopping cart
clean up products 53
delete 53, 57
display 53
empty 53
fill 50
give reason 55
manage 52
move product to another shelf 66
request for multiple identities 56
save for later 66
saved for later 66-69
set validity period 54
specify priority 55
submit 53
specify priority 55
start page 28
structure 27
submit
shopping cart 53
subscription
manage 25
system entitlements
make requestable 189
manage 157, 188
prepare for request 189
system roles
manage 128

U
user accounts
manage 187
user interface 27

V
value format 24