One Identity Manager 9.3

IT Shop Administration Guide

Copyright 2025 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 website (http://www.OneIdentity.com) for regional and international office information.

Patents

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

Trademarks

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

Legend

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

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

One Identity Manager IT Shop Administration Guide
Updated - 06 January 2025, 10:20

For the most recent documents and product information, see Online product documentation.

Contents

Setting up an IT Shop solution **11**
One Identity Manager users in the IT Shop 12
Implementing the IT Shop 14
Using the IT Shop with the Application Governance Module 16
Requestable products 16
Multi-request resources 19
Preparing products for requesting 21
Entering service items 22
General main data for service items 23
Pricing for service items 26
Extended main data for service items 27
Default service items 27
Specifying dependencies between products 27
Editing product dependencies for requests 28
Defining hierarchy for service items 29
Assigning hierarchical roles to service items 29
Assigning functional areas to service items 31
Assigning extended properties to service items 31
Displaying websites for service items 32
Changing products for service items 32
Adding tags and assigning them to service items 33
Displaying the service item overview 34
Reports about service items 34
Entering service categories 36
Main data for service categories 36
Default service categories 38
Assigning service items to service categories 39
Displaying the service category overview 39
Entering product-specific request properties 40
Request property and request parameter settings 41
Copy request properties 47

Displaying the request properties overview ... 48
Products for requests with time restrictions ... 48
Product request on customer or product relocation ... 49
Non-requestable products ... 50
Entering terms of use for service items ... 50
Assigning files to terms of use ... 51
Displaying the terms of use overview ... 52
Entering tags ... 52
Assigning service items to tags ... 53
Displaying the tags overview ... 54
Assigning and removing products ... 54
Assigning products to shelves ... 56
Removing products from shelves ... 57
Moving products to another shelf ... 57
Replacing products ... 58
Preparing the IT Shop for multi-factor authentication ... 59
Assignment requests ... 60
Standard products for assignment requests ... 60
Requesting memberships in business roles ... 62
Requesting memberships in application roles ... 63
Customizing assignment requests ... 64
Canceling requests ... 65
Removing customers from a shop ... 66
Setting up assignment resources ... 67
General main data for assignment resources ... 68
Default assignment resources ... 69
Displaying assignment resource overviews ... 70
Adding assignment resources to the IT Shop ... 70
Removing assignment resources from the IT Shop ... 70
Delegations ... 71
Standard products for delegation ... 72
Preparing single delegations ... 73
Allowing delegation approvals ... 74
Creating IT Shop requests from existing user accounts, assignments, and role memberships ... 75

Creating requests for identities ... 76
Creating user account requests ... 77
Creating workdesk requests ... 78
Creating assignment requests ... 80
Adding system entitlements automatically to the IT Shop ... 81
Deleting unused application roles for product owners ... 83

Approval processes for IT Shop requests ... 85
Approval policies for requests ... 85
General main data of approval policies ... 86
Default approval policies ... 87
Adding to the IT Shop ... 88
Validity checking ... 88
Editing approval workflows ... 88
Copying approval policies ... 89
The approval policy overview ... 90
Approval workflows for requests ... 90
Working with the Workflow Editor ... 90
Setting up approval workflows ... 93
Editing approval levels ... 94
Editing approval steps ... 95
Properties of an approval step ... 95
Connecting approval levels ... 101
Copying approval workflows ... 101
Deleting approval workflows ... 102
The approval workflow overview ... 102
Default approval workflows ... 103
Determining effective approval policies ... 103
Approvers for renewals ... 104
Approvers for unsubscriptions ... 105
Selecting responsible approvers ... 105
Default approval procedures ... 105
Determining request recipients as approvers ... 108
Determining managers or members of a role as approvers ... 108
Determining owners as approvers ... 110
Determining special approvers ... 113

Determining target system managers as approvers ... 117
Determining requester or recipients ... 118
Determining special identities as approvers ... 118
Automatic approvals ... 119
Setting up approval procedures ... 125
General main data of an approval procedure ... 126
Queries for determining approver ... 126
Copying an approval procedure ... 129
Deleting approval procedures ... 130
Determining the responsible approvers ... 130
Request risk analysis ... 132
Testing requests for rule compliance ... 133
Compliance checking requests ... 134
Identifying rule violations ... 136
Determining exception approvers ... 136
Restricting exception approvers ... 139
Setting up exception approver restrictions ... 140
Explicit exception approval ... 141
Rule checking for requests with self-service ... 142
Approving requests from an approver ... 142
Setting up approver restrictions ... 144
Automatically approving requests ... 144
Configuring automatic approval ... 146
Approval by peer group analysis ... 147
Configuring peer group analysis for requests ... 148
Approval recommendations for requests ... 149
Criteria for approval recommendations for requests ... 150
Configuring approval recommendations for requests ... 152
Gathering further information about a request ... 154
Appointing other approvers ... 154
Escalating an approval step ... 155
Approvers cannot be established ... 157
Automatic approval on timeout ... 159
Halting a request on timeout ... 160
Approval by the chief approval team ... 161

Approving requests with terms of use ... 163
Using default approval processes ... 164

Request sequence ... 167
The request overview ... 169
Displaying request details ... 169
Displaying the approval sequence ... 169
Displaying the approval history ... 170
Requesting products more than once ... 171
Requests with limited validity period ... 172
Renewing requests ... 173
Canceling or unsubscribing requests ... 174
Checking request validity periods ... 174
Relocating a customer or product to another shop ... 176
Changing approval workflows of pending requests ... 176
Requests for employees ... 178
Requesting change of manager for an employee ... 178
Canceling requests ... 180
Unsubscribe products ... 181
Notifications in the request process ... 181
Requesting approval ... 182
Reminding approvers ... 182
Scheduled request for approval ... 184
Sequence for limited requests ... 184
Approving or denying request approval ... 185
Notifying delegates ... 185
Canceling requests ... 187
Escalating requests ... 187
Delegating approvals ... 188
Rejecting approvals ... 188
Notifications with questions ... 188
Using additional approvers to approve requests ... 189
Unsubscribing approved requests ... 190
Renewing approved requests ... 190
Product change notifications ... 190
Default mail templates ... 191

Bulk delegation notifications ... 191
Approval by mail ... 191
Editing approval emails ... 194
Adaptive cards approval ... 195
Using adaptive cards for approvals ... 196
Adding and deleting recipients and channels ... 197
Creating, editing, and deleting adaptive cards for requests ... 198
Creating, editing, and deleting adaptive cards templates for requests ... 200
General main data for adaptive cards ... 201
Deploying and evaluating adaptive cards for requests ... 202
Disabling adaptive cards ... 202
Requests with limited validity period for changed role memberships ... 203
Requests from permanently deactivated identities ... 204
Deleting request procedures and deputizations ... 205

Managing an IT Shop ... 206
IT Shop base data ... 206
Processing status ... 208
Standard reason for requests ... 209
Predefined standard reasons for requests ... 210
Role classes for the IT Shop ... 211
Role types for the IT Shop ... 212
Business partners ... 212
Functional areas ... 214
Chief approval team ... 215
Product owners ... 216
Attestors ... 217
Setting up IT Shop structures ... 218
Adding IT Shop structures ... 219
General main data of IT Shop structures ... 219
Custom main data of IT Shop structures ... 221
Assigning approval policies ... 222
Assigning requestable products to shelves ... 222
The IT Shop structure overview ... 223
Setting up a customer node ... 223
Adding customer nodes ... 224

General main data of customer nodes ... 224
Custom main data of customer nodes ... 225
Assigning identities directly ... 225
Assigning identities through dynamic roles ... 226
The entitled customers overview ... 227
Deleting IT Shop structures ... 228
Deleting customer nodes ... 228
Deleting shelves ... 228
Deleting shops ... 229
Deleting shopping centers ... 230
Restructuring the IT Shop ... 230
Moving shops to other shopping centers ... 231
Moving shelves to other shops ... 231
Moving products to another shelf ... 231
Templates for automatically filling the IT Shop ... 232
Using shelf templates in an IT Shop solution ... 236
Editing shelf templates ... 237
General main data of a shelf template ... 237
Custom main data of shelf templates ... 238
Assigning approval policies ... 238
Assigning requestable products to shelf templates ... 239
Shelf-filling wizard ... 240
Assigning shelf templates to shops and shopping center templates ... 240
Deleting shelf templates ... 241
Custom mail templates for notifications ... 243
Creating and modifying IT Shop mail templates ... 243
General properties of mail templates ... 244
Creating and editing mail definitions ... 245
Using base object properties ... 246
Use of hyperlinks to the Web Portal ... 247
Default functions for creating hyperlinks ... 248
Customize email signatures ... 249
Copying IT Shop mail templates ... 250
Displaying IT Shop mail template previews ... 250
Deleting IT Shop mail templates ... 250

Custom notification processes 251
Product bundles 251
Creating and modifying product bundles 251
General main data of a product bundle 252
Cart items 253
Deleting product bundles 253
Recommendations and tips for transporting IT Shop components with the Database Transporter 254
Troubleshooting errors in the IT Shop 255
Timeout on saving requests 255
Bulk delegation errors 256
Process monitoring for requests 256
Appendix: Configuration parameters for the IT Shop 258
Appendix: Request statuses 273
Appendix: Examples of request results 275
Appendix: Example of defining request properties 278
About us 279
Contacting us 279
Technical support resources 279
Index 280

1

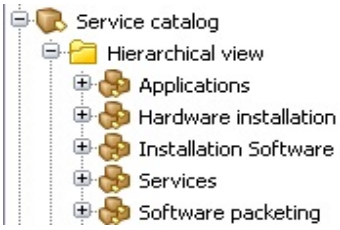
Setting up an IT Shop solution

The IT Shop allows users to request company resources such as software, system roles, or group membership as well as non-IT resources such as mobile telephones or keys. Furthermore, membership of a hierarchical role (department, location, cost center, or business role) can be requested through the IT Shop. The requests are processed by a flexible policy-based approval process. Introducing the IT Shop avoids time-consuming demands within the company and reduces the administration effort. The request history makes it possible to follow who requested which company resource or hierarchical role and when it was requested, renewed, or canceled.

Shops, shelves, customers, and products all belong to an IT Shop solution. Several shops can be grouped together into shopping centers. The shelves are assigned company resources in the form of products. Products can be grouped into service categories. All the service categories are summarized in a service catalog. Customers can select products from a service catalog in the Web Portal, add them to a cart, and send a purchase request.

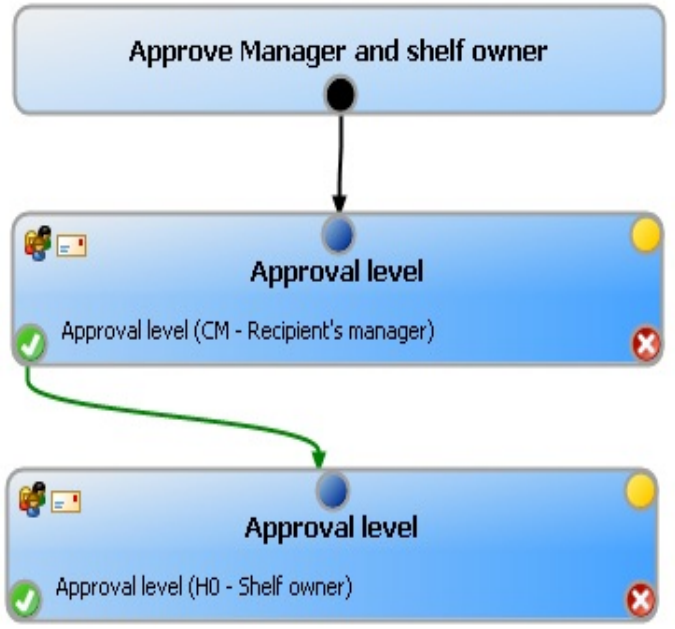
The following figure shows an example of a service catalog with service categories.

Figure 1: Example of a service catalog



Requests follow a defined approval process that determines whether a product may be assigned or not. Products can be renewed or canceled. Approval processes can also be specified for renewals and cancellations. Approval policies are defined for approval processes. The approval policies are assigned to approval workflows for product requests, renewals, or cancellations.

Figure 2: Example of a simple approval workflow



The products are requested, renewed, and canceled through the Web Portal. Authorized identities have the option to approve requests and cancellations. For more information about this, see the *One Identity Manager Web Portal User Guide*.

One Identity Manager users in the IT Shop

The following users are involved in the setting up and operating of an IT Shop system.

Table 1: Users

Users	Tasks
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role: • Create the IT Shop structure with shops, shelves, customers, templates, and service catalog. • Create approval policies and approval workflows. • Specify which approval procedure to use to find attestors. • Create products and service items.

Users	Tasks
	• Set up request notifications. • Monitor request procedures. • Administrate application roles for product owners and attestors. • Maintain members of the chief approval team. • Set up other application roles as required. • Create extended properties for company resources of any type. • Edit the resources and assign them to IT Shop structures. • Assign system entitlements to IT Shop structures.
Product owners	Product owners must be assigned to the **Request & Fulfillment | IT Shop | Product owners** application role or a child application role. Users with this application role: • Approve through requests. • Edit service items and service categories under their management.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles. One Identity Manager administrators: • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required.
Role approver	• Request approval in the Web Portal. Approvers are determined through approval processes.
Attestors for requests	Attestors must be assigned to the **Request & Fulfillment | IT Shop | Attestors** application role.

Users	Tasks
	Users with this application role: • Attest correct assignment of company resource to IT Shop structures for which they are responsible. • Attest objects that have service items assigned to them. • Can view main data for these IT Shop structures but not edit them. NOTE: This application role is available if the Attestation Module is installed.
Chief approval team	Chief approvers must be assigned to the **Request & Fulfillment | IT Shop | Chief approval team** application role. Users with this application role: • Approve through requests. • Assign requests to other approvers.

Implementing the IT Shop

Identity & Access Lifecycle is already included in the default installation of One Identity Manager. This shop contains several shelves that have standard products assigned to them. You can use these products to request role or group memberships, for example, or to delegate duties. All active identities automatically become members of this shop and can therefore make requests.

You can use the **Identity & Access Lifecycle** shop to request standard products. Default approval policies are implemented for approving these requests. You can request any company resources you like by taking the default shop and extending it with your own shelves or by setting up your own IT Shop solution.

To use the Identity & Access Lifecycle shop

1. In the Designer, set the **QER \| ITSHOP** configuration parameter.

   In the default installation, the configuration parameter is set and the IT Shop is available. If the configuration parameter is not set, you can set it in the Designer and then compile the database.

   If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

2. Install and configure the Web Portal.

The products are requested, renewed, and canceled through the Web Portal. Authorized identities have the option to approve requests and cancellations.

For more information about this, see the *One Identity Manager Installation Guide* and the *One Identity Manager Web Portal User Guide*.

To customize the Identity & Access Lifecycle shop

1. Set up more shelves.

   For more information, see Managing an IT Shop on page 206.

2. Prepare company resources for requesting.

   For more information, see Preparing products for requesting on page 21.

3. Assign requestable products to the shelves.

   For more information, see Assigning and removing products on page 54.

4. Set up the approval process.

   In the default installation, different default approval policies are assigned to the **Identity & Access Lifecycle** shop. Therefore, requests from this shop are run through predefined approval processes.

   You can also assign your own approval policy to the shop. For more information, see Approval processes for IT Shop requests on page 85.

5. If necessary, edit the dynamic role condition.

   For more information, see Assigning identities through dynamic roles on page 226. For more information about creating the condition, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To set up your own IT Shop solution

1. In the Designer, set the **QER | ITSHOP** configuration parameter.

   In the default installation, the configuration parameter is set and the IT Shop is available. If the configuration parameter is not set, you can set it in the Designer and then compile the database.

   If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

2. Set up shops, shelves, and customer node.

   For more information, see Managing an IT Shop on page 206.

3. Prepare company resources for requesting.

   For more information, see Preparing products for requesting on page 21.

4. Assign requestable products to the IT Shop.

   For more information, see Assigning and removing products on page 54.

One Identity Manager makes different standard products available, which can be requested through the **Identity & Access Lifecycle** shop. You can also add these standard products to your own IT Shop.

5. Set up the approval process.

   For more information, see Approval processes for IT Shop requests on page 85.

6. Install and configure the Web Portal.

   The products are requested, renewed, and canceled through the Web Portal. Authorized identities have the option to approve requests and cancellations.

   For more information, see the *One Identity Manager Installation Guide* and the *One Identity Manager Web Portal User Guide*.

Related topics

- Using the IT Shop with the Application Governance Module on page 16

Using the IT Shop with the Application Governance Module

The Application Governance Module allows you to quickly and simply run the onboarding process for new applications from one place. An application created with the Application Governance Module combines all the entitlements application users require for their regular work. This way, you can assign application entitlements to your applications (such as system entitlements or system roles) and plan when they will be available as requestable products (service items) in the Web Portal, for example.

For more information about the Application Governance Module, see the *One Identity Manager Application Governance User Guide*. For more information about configuring the Application Governance Module, see the *One Identity Manager Web Application Configuration Guide*.

Applications can also be set up in the Manager if the Application Governance Module is available. For more information about the main data of applications and application entitlements, see the *One Identity Manager Application Governance User Guide*.

Requestable products

Requestable products in the IT Shop are company resources such as target system groups, software, and non-IT resources after they have been assigned to a shelf. The following company resources can be assigned to shelves as requestable products.

Table 2: Requestable products

Company resource	Available in module	Documentation guide
Groups and system entitlements of custom target systems	Target System Base Module	One Identity Manager Target System Base Module Administration Guide
Active Directory groups	Active Directory Module	One Identity Manager Administration Guide for Connecting to Active Directory
SharePoint groups and SharePoint roles	SharePoint Module	One Identity Manager Administration Guide for Connecting to SharePoint
HCL Domino groups	Domino Module	One Identity Manager Administration Guide for Connecting to HCL Domino
LDAP groups	LDAP Module	One Identity Manager Administration Guide for Connecting to LDAP
SAP groups, SAP roles, and SAP profiles	SAP R/3 User Management Module	One Identity Manager Administration Guide for Connecting to SAP R/3
SAP structural profiles	SAP R/3 Structural Profiles Add-on Module	One Identity Manager Administration Guide for SAP R/3 Structural Profiles Add-on
SAP BI analysis authorizations	SAP R/3 Analysis Authorizations Add-on Module	One Identity Manager Administration Guide for SAP R/3 Analysis Authorizations Add-on
E-Business Suite permissions	Oracle E-Business Suite Module	One Identity Manager Administration Guide for Connecting to Oracle E-Business Suite
Microsoft Entra ID group, Microsoft Entra ID administrator roles, Microsoft Entra ID role assignments,	Microsoft Entra ID Module	One Identity Manager Administration Guide for Connecting to Microsoft Entra ID

Company resource	Available in module	Documentation guide
Microsoft Entra ID role permissions		
Google Workspace groups, Google Workspace products and SKUs, Google Workspace Admin role assignments	Google Workspace Module	One Identity Manager Administration Guide for Connecting to Google Workspace
Cloud groups and system entitlements	Cloud Systems Management Module	One Identity Manager Administration Guide for Connecting to the Universal Cloud Interface
PAM user groups	Privileged Account Governance Module	One Identity Manager Administration Guide for Privileged Account Governance
OneLogin roles	OneLogin Module	One Identity Manager Administration Guide for Integration with OneLogin Cloud Directory
API key requests, file requests, password requests, remote desktop application requests, remote desktop session requests, SSH key requests, SSH session requests, and Telnet session requests.	Privileged Account Governance Module	One Identity Manager Administration Guide for Privileged Account Governance
Resources	Identity Management Base Module	One Identity Manager Identity Management Base Module Administration Guide
Multi-request resources	Identity Management Base Module	One Identity Manager

Company resource	Available in module	Documentation guide
		Identity Management Base Module Administration Guide
Account definitions	Target System Base Module	One Identity Manager Target System Base Module Administration Guide
System roles	System Roles Module	One Identity Manager System Roles Administration Guide
Subscribable reports	Report Subscription Module	One Identity Manager Report Subscriptions Administration Guide
Software	Software Management Module	One Identity Manager Software Management Administration Guide
Assignment resources	Identity Management Base Module Business Roles Module	Use assignment resources to request any number of assignments to hierarchical roles or to delegate responsibilities through the IT Shop. One Identity Manager IT Shop Administration Guide, Assignment requests on page 60

Software and system roles can also be requested for workdesks. The request's `UID_Workdesk` is given as additional information here (`PersonWantsOrg.UID_WorkdeskOrdered`).

Multi-request resources

The IT Shop distinguishes between single or multiple requestable products. Single request products are, for example, software, system roles, or Active Directory groups. These products cannot be requested if they have already been be requested for the same time period.

Furthermore, there may be company resources that are needed more than once, consumables, for example. You can find company resources such as these mapped in One Identity Manager as **Multi-request resource** or **Multi requestable/unsubscribable resources**.

Table 3: Resource types

Type	Description	Table
Resources	Resources that an identity (workdesk, device) may own just once. The resources can be requested in the IT Shop just once. The resources are assigned to the identities after approval has been granted. They remain assigned until the request is unsubscribed. You can request them again a later point. Example: phone, company car.	QERResource
Multi-request resources	Resources that can be requested more than once in the IT Shop. Requests are automatically canceled once approved. The resources are not explicitly assigned to identities. Example: resource for requesting remote desktop sessions for assets in a PAM system; consumables, such as pens, printing paper.	QERReuse
Multi requestable/unsubscribable resources	Resources that an identity can request more than once in the IT Shop but must return them explicitly once they are no longer needed. The resources are assigned to the identities after approval has been granted. They remain assigned until the request is canceled. Example: printer, monitor, Microsoft Entra ID role assignment	QERReuseUS

To set up multi-request resources and add them as products in the IT Shop

1. In the Manager, select the **Entitlements > Multi-request resources for IT Shop** category.
2. Click in the result list.
3. Edit the resource's main data.
4. Save the changes.
5. Select the **Add to IT Shop** task.
    - To assign the resource to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, select the shelves with a double-click.

- To assign the resource to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, select the template with a double-click.

TIP: In the **Remove assignments** pane, you can remove shelf assignments.

To remove an assignment

- Select the shelf and double-click ✓.

6. Save the changes.

To set up multi requestable/unsubscribable resources and to add them as products to the IT Shop

1. In the Manager, select the **Entitlements > Multi requestable/unsubscribable resources for IT Shop** category.
2. Click ✚ in the result list.
3. Edit the resource's main data.
4. Save the changes.
5. Select the **Add to IT Shop** task.
   - To assign the resource to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, select the shelves with a double-click.
   - To assign the resource to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, select the template with a double-click.

TIP: In the **Remove assignments** pane, you can remove shelf assignments.

To remove an assignment

- Select the shelf and double-click ✓.

6. Save the changes.

For more information about multi requestable products, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Preparing products for requesting

Company resources have to fulfill at least the following prerequisites before you can request them in the Web Portal:

- The company resource must be labeled with the **IT Shop** option.
- A service item must be assigned to the company resource.
- The company resource must be assigned to a shelf as a product.
- If the company resource is only assigned to identities using IT Shop requests, the company resource must also be labeled with the **Only use in IT Shop** option. This

means that the company resource cannot be directly assigned to roles outside the IT Shop.

The **Entitlements** category displays all company resources that can be requested using the IT Shop. This includes software, system entitlements, system roles, account definitions, resources, multi-request resources, and assignment resources if the corresponding modules are installed.

You can prepare the company resources for requesting in the IT Shop if you are an IT Shop administrator and have logged in as role-based. You can assign service items, edit the **IT Shop** and **Only use in IT Shop** options and assign the company resources to IT Shop shelves.

To prepare company resources for requesting

1. In the Manager, select the **Permissions** category.
2. Navigate to the result list and select the company resource you want.
3. Select the **Change main data** task.
4. Enable the **IT Shop** option.
5. Assign a new service item in the **Service item** field.

   To add a new service item, click . Copy the name of the company resource as identifier for the service item. Enter the other properties on the service item main data form.
6. Save the changes.
7. Select the **Add to IT Shop** task.
8. In the **Add assignments** pane, assign the company resource to shelves.
9. Save the changes.

Customer keep their requested products on the shelf until they unsubscribe them. Sometimes, however, products are only required for a certain length of time and can be canceled automatically after this time. There are other settings required to provide limited period products.

Detailed information about this topic

- Entering service items on page 22
- Products for requests with time restrictions on page 48

Entering 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 the company resources. For example, you can specify article numbers, request properties, product supervisors, or approvers for requests. A service catalog can be put together from the service items the

Web Portal. These contain all the requestable products. You can use service categories, tags, and service item names to find the product in the service catalog.

To create or edit service categories

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. In the result list, select the product's service item and select the **Change main data** task.

   - OR -

   Click in the result list.
3. Enter the service item's main data.
4. Save the changes.

General main data for service items

Enter the following general main data. If you add a new service item, you must fill out the required fields.

Table 4: General main data of a service item

Main data	Meaning
Service item	Service item name.
Special service item	If a product is used for a specific purpose, for example, for product collection, then mark it as a special service item.
Service category	Group individual products into a collection of products. Select an existing service category from the list or add a new one. To create a new service category, click . Enter at least one name for the service item.
Product owners	Assign a **Request & Fulfillment | IT Shop | Product owner** application role. Product owners can be used as approvers in a defined approval process within the IT Shop. They can decide on approval of the service item request. To create a new application role, click . Enter the application role name and assign a parent application role. If no product owner is assigned, the product owner of the assigned service category is determined by template.

Main data	Meaning
Attestors	Assign a **Request & Fulfillment | IT Shop | Attestor** application role. The members of this application role can chosen as attestor in an attestation procedure. To create a new application role, click . Enter the application role name and assign a parent application role.
Cost center	Cost center for booking the service item in the accounts.
Manufacturer	Manufacturer data.
Terms of use	Terms of use for the product. The product can only be requested if the requester has accepted the terms of use.
Request number, product code, product code (foreign)	Company-specific service item properties.
Functional area	Company-specific service item property.
Approval policies	Approval policy used to determine the approver when the service item is requested in the IT Shop.
Request property	Select a request property using the additional request parameters that are defined for a request. 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. To create a new request property, click and enter the request property's name. Then define the request parameters.
Calculation info	Enter the calculation mode as accounting information.
Availability	Company-specific information about the service item‘s availability.
Sort order	Customer-specific criteria for sorting service items.
Website	Web page with more information about the service item. This field allows you to link product descriptions in the internet or intranet to the service item. To open the website, select **Visit website** in the default web browser.
Validity period	Time period for limited assignments through IT Shop. The service item is automatically canceled when the time expires. When multi-request resources are requested (`QERReuse`), this value has

Main data	Meaning
	no effect. Changing the deadline will not affect requests that have already been approved. The new deadline applies to new requests. It is taken into account when calculating the expiration date of pending request if no deadline was previously set (value change from **0** to greater than **0**).
Reason type on request	Specifies which type of reason is required when requesting this service item. • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on approval	Specifies which type of reason is required when granting approval to this service item. • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on denial	Specifies which type of reason is required when denying approval to this service item. • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Description	Text field for additional explanation.
Retain service item assignment on relocation	Specifies whether requests belonging to this service item remain intact when a customer or a product relocates.
Request parameters must be defined per recipient	Specifies whether request parameters must be entered separately for each recipient of this product, if the product is requested for different recipients in one request procedure. If this option is not set, the selected request parameters apply uniformly to all recipients of the product.
Not available	Specifies whether the service item can still be requested in the IT Shop.

Main data	Meaning
	If this option is enabled, no new requests can be placed for this item. Existing requests remain intact.
Hide in service catalog	Specifies whether the service item is shown in the service catalog. If the option is set, the service item can be requested, but it is not displayed in the service catalog.
Approval by multi-factor authentication	The approval of requests with this service item requires multi-factor authentication.

For more information about attestation, see the *One Identity Manager Attestation Administration Guide*. For more information about cost centers, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Detailed information about this topic

- Entering service categories on page 36
- Selecting responsible approvers on page 105
- Product owners on page 216
- Attestors on page 217
- Business partners on page 212
- Functional areas on page 214
- Determining effective approval policies on page 103
- Entering product-specific request properties on page 40
- Products for requests with time restrictions on page 48
- Product request on customer or product relocation on page 49
- Moving products to another shelf on page 231
- Entering terms of use for service items on page 50
- Preparing the IT Shop for multi-factor authentication on page 59

Pricing for service items

Enter the required pricing information for booking the service item to the accounts on the **Calculation** tab.

Table 5: Pricing for a service item

Property	Description
Purchase price	Purchase price.
Sales price	Sales price.
Internal price	Internal transfer price.
Rental rate (purchasing)	Purchase price on product rental.
Rental rate (selling)	Sales price on product rental
Rental rate (internal)	Internal transfer price on product rental
Currency	Currency unit
Sales tax	Sale tax to apply in percent (%)

Extended main data for service items

On the **Picture** tab, you can import an image of the product into the data base. Select the path where the picture is stored.

On the **User-defined** tab, enter additional company-specific information in the spare fields. Use the Designer to customize display names, formats, and templates for the fields.

Default service items

One Identity Manager provides service items by default. These service items are assigned to the **Identity & Access Lifecycle** shop. You can request them as standard products through the Web Portal.

To edit default service items

- In the Manager, select the **IT Shop > Service catalog > Predefined** category.

Specifying dependencies between products

You can define dependencies for products. For example, when a printer is requested, a flat-rate installation charge has to be requested at the same time, and toner may be requested optionally. You can also specify if two products should never be requested simultaneously.

Dependencies between requestable products are created using service items.

When a product is requested, it is tested for dependencies and in this case, dependent products are added to the request.

To specify dependencies between products

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the product's service item in the result list.
3. Select the **Edit product dependencies for requests** task.
   - In the **Dependent products** tab, specify the dependent products.

     In the **Add assignments** pane, assign the service items.
   - In the **Depends on products** tab, specify which selected service item is dependent on which products.

     In the **Add assignments** pane, assign the service items.
4. Save the changes.
5. Select the **Service item overview** task.
6. Define the properties of the product dependency.
   a. On the **Dependent products** or **Depends on products** form element, select the dependent product.

      This opens the product dependency details form.
   b. Specify the dependency conditions. Select one of the following options:
      - Cannot request products together

        This option prevents the dependent product from being acquired by the same request. The product can be assigned at any time with a separate, direct request.
      - Product must be requested at the same time
      - Product can optionally be requested with another
7. Save the changes.

Editing product dependencies for requests

Dependencies between products are taken into account by Web Portal requests.

Detailed information about this topic

- Specifying dependencies between products on page 27

Defining hierarchy for service items

You can structure service items hierarchically. To do this, assign a service item below or above another service item.

To structure service items hierarchically

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. In the result list, select a service item in the result list and run the task **Edit service item hierarchy**.
3. Select the **Child service items** tab.

   In the **Add assignments** pane, assign child service items.

   TIP: In the **Remove assignments** pane, you can remove service item assignments.

   To remove an assignment

   - Select the service item and double-click ✓.
4. Select the **Parent service items** tab.

   In the **Add assignments** pane, assign parent service items.

   TIP: In the **Remove assignments** pane, you can remove service item assignments.

   To remove an assignment

   - Select the service item and double-click ✓.
5. Save the changes.

Assigning hierarchical roles to service items

You can use One Identity Manager to assess the risk of assignments. The assessments can be evaluated separately by role. Prerequisite is that service items are assigned to the roles. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Assigning organizations to service items

To assign a service item to departments, cost centers, and locations

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the service item in the result list.
3. Select the **Assign organizations** task.

   In the **Add assignments** pane, assign the organizations:

   - On the **Departments** tab, assign departments.
   - On the **Locations** tab, assign locations.
   - On the **Cost centers** tab, assign cost centers.

   TIP: In the **Remove assignments** pane, you can remove assigned organizations.

   To remove an assignment

   - Select the organization and double-click .
4. Save the changes.

Assigning business roles to service items

NOTE: This function is only available if the Business Roles Module is installed.

You can issue separate invoices according to the different company structures. Assign service items to business roles to do this.

To assign service items to business roles

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the service item in the result list.
3. Select the **Assign business roles** task.

   In the **Add assignments** pane, select the role class and assign business roles.

   TIP: In the **Remove assignments** pane, you can remove assigned business roles.

To remove an assignment

- Select the business role and double-click ✓.

4. Save the changes.

Assigning functional areas to service items

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*.

To assign functional areas to a service item

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the service item in the result list.
3. Select the **Assign functional areas** task.

   Assign the functional areas in **Add assignments**.

   TIP: In the **Remove assignments** pane, you can remove functional area assignments.

   To remove an assignment

   - Select the functional area and double-click ✓.
4. Save the changes.

Related topics

- Approval by peer group analysis on page 147

Assigning extended properties to service items

Extended properties are meta objects, such as operating codes, cost codes, or cost accounting areas that cannot be mapped directly in One Identity Manager.

To assign extended properties to a service item

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.

2. Select the service item in the result list.
3. Select the **Assign extended properties** task.

   In the **Add assignments** pane, assign extended properties.

   TIP: In the **Remove assignments** pane, you can remove assigned extended properties.

   To remove an assignment

   - Select the extended property and double-click ✓.
4. Save the changes.

Displaying websites for service items

You can link product descriptions in internet or intranet with the service item. For this, you enter the URL of a website in **Website** on the main data form.

To open the website in a standard browser

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the service item in the result list.
3. Select the **Visit website** task.

Related topics

- General main data for service items on page 23

Changing products for service items

A product can be replaced by another product at a specified time. All identities who have requested this product are notified by an email telling them to request a replacement product.

To replace a product with another one

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.

2. Select the product's service item to replace in the result list.
3. Select the **Change product** task.
4. Enter the following data:
    - **Expiry date**: Date on which the product is replaced by a different product.
    - **Alternative product**: Service item that can be requested instead.
5. Click **OK**.

Related topics

- Product change notifications on page 190

Adding tags and assigning them to service items

Use this task to assign tags to service items and to add new tags.

To add and assign a tag to a service item

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the service item in the result list.
3. Select the **Assign tag** task.
4. Select the **Create tag** task.
5. Enter the tag and a description for it.
6. Save the changes.

   The new tag is shown on the assignment form.
7. Double-click on the tag to assign it to the selected service item.
8. Save the changes.

To assign a tag to a service item

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the service item in the result list.

3. Select the **Assign tag** task.

   In the **Add assignments** pane, assign the tag.

   TIP: In the **Remove assignments** pane, you can remove assigned tag.

   To remove an assignment

   - Select the tag and double-click ✓.

4. Save the changes.

TIP: You can add more tags. For more information, see Entering tags on page 52.

Displaying the service item overview

On the overview form, you can see the most important information about a service item.

To obtain an overview of a service item

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.

2. Select the service item in the result list.
3. Select the **Service item overview** task.

Reports about service items

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for service items.

NOTE: Other sections may be available depending on the which modules are installed.

Table 6: Reports about service items

Report	Description
Overview of all assignments	This report finds all roles containing identities with the selected service item.

Related topics

- Overview of all assignments on page 35

Overview of all assignments

The **Overview of all assignments** report is displayed for some objects, such as authorizations, compliance rules, or roles. The report finds all the roles, for example, departments, cost centers, locations, business roles, and IT Shop structures in which there are identities who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Example: Assignment overview

- If the report is created for a resource, all roles are determined in which there are identities with this resource.
- If the report is created for a group or another system entitlement, all roles are determined in which there are identities with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are identities who violate this compliance rule.
- If the report is created for a department, all roles are determined in which identities of the selected department are also members.
- If the report is created for a business role, all roles are determined in which identities of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the **Overview of all assignments** report.
- Click the **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain identities with the selected base object.

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are identities with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the icon in the report's toolbar.
- Double-click a control to show all child roles belonging to the selected role.
- By clicking the button in a role's control, you display all identities in the role with the base object.
- Use the small arrow next to to start a wizard that allows you to bookmark this list of identities for tracking. This creates a new business role to which the identities are assigned.

Figure 3: Toolbar of the Overview of all assignments report.

Table 7: Meaning of icons in the report toolbar

Icon	Meaning
	Show the legend with the meaning of the report control elements
	Saves the current report view as a graphic.
	Selects the role class used to generate the report.
	Displays all roles or only the affected roles.

Entering service categories

You can group individual service items into service categories to create a service catalog.

To edit service categories

1. In the Manager, select the **IT Shop > Basic configuration data > Service categories** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog** category.
2. In the result list, select the service category and run the **Change main data** task.
3. Edit the service category's main data.
4. Save the changes.

Main data for service categories

Enter the following main data of a service category. If you add a new service category, you must fill out the required fields.

Table 8: General main data of a service category

Main data	Meaning
Service category	The service item’s name.
Special service category	Specifies whether the service category has a special purpose.
Parent service category	If you want to have service categories in a hierarchical structure, select a parent service category from the list.
Product	Assign a **Request & Fulfillment | IT Shop | Product owner** applic-

Main data	Meaning
owners	ation role. Product owners can be used as approvers in a defined approval process within the IT Shop. They can decide on approval of the service item request. To create a new application role, click . Enter the application role name and assign a parent application role.
Attestors	Assign a **Request & Fulfillment | IT Shop | Attestor** application role. The members of this application role can chosen as attestor in an attestation procedure. To create a new application role, click . Enter the application role name and assign a parent application role. For more information, see the *One Identity Manager Attestation Administration Guide*.
Approval policies	Approval policies used to determine the approver when the service item is requested from a service category in the IT Shop.
Request property	Select a request property using the additional request parameters that are defined for a request. 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. To create a new request property, click and enter the request property's name. Then define the request parameters.
Purchase price, sales price, internal price, currency	Enter the required price information for the service category accounting.
Sort order	Customer specific criteria for sorting assigned service items.
Reason type on request	Specifies which type of reason is required when requesting a service item from this service catalog. • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type	Specifies which type of reason is required when granting approval to a

Main data	Meaning
on approval	service item from this catalog. • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on denial	Specifies which type of reason is required when denying approval to a service item from this catalog. • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Description	Text field for additional explanation.
Full name	Full name of the service category.
Remarks	Text field for additional explanation.
Picture	Picture for this service category. Select the path where the picture is stored.
Spare field no. 01 - spare field no. 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Detailed information about this topic

- Selecting responsible approvers on page 105
- Product owners on page 216
- Attestors on page 217
- Determining effective approval policies on page 103
- Entering product-specific request properties on page 40

Default service categories

One Identity Manager provides service categories by default. These service categories make up the default service items in the service catalog.

To edit default service categories

- In the Manager, select the **IT Shop > Basic configuration data > Service categories > Predefined** category.

Assigning service items to service categories

Use this task to assign any number of service items to a service category.

To assign service items to a service category

1. In the Manager, select the **IT Shop > Basic configuration data > Service categories** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog** category.
2. Select the service category in the result list.
3. Select the **Assign service items** task.

   In the **Add assignments** pane, assign service items.

   TIP: In the **Remove assignments** pane, you can remove service item assignments.

   To remove an assignment

   - Select the service item and double-click .
4. Save the changes.

Displaying the service category overview

The overview form, shows you the most important information about a service category, at a glance.

To obtain an overview of a service category

1. In the Manager, select the **IT Shop > Basic configuration data > Service categories** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog** category.
2. Select the service category in the result list.
3. Select the **Service category overview** task.

Entering product-specific request properties

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.

Define a request parameter for each feature of a request property. Parameters can be marked as mandatory if a value must be entered when they are requested.

To be able to use request properties, you assign them to service items or service categories. When a product is requested, the parameters of this request property are displayed. If a service item does not have a request property assigned to it, the service category's request property is used. If a service category does not have a request property assigned to it, the parent service category's request property applies.

NOTE: The definition of request properties was redesigned with One Identity Manager version 8.2. Now you can define a lot of additional information for request parameters. This makes the implementation of request properties more flexible. The previous solution can still be used. When you add a new request property, you specify whether you want to use the obsolete or the new style definition.

Adding request properties with the new style definition

To add a request property

1. In the Manager, select the **IT Shop > Basic configuration data > Request properties** category.
2. Click in the result list.
3. Enter the name and a description for the request property.

   Leave the **Obsolete definition** option disabled. After saving, the option cannot be changed again.
4. Save the request property.
5. Select the **Parameter** tab.
6. Click **Add**.
7. Edit the request parameter's main data.
8. To add another request parameter, click **Add**.
9. Save the changes.
10. Recompile the database if the scripts for calculating values have been changed in the parameter settings.

Adding request properties with the obsolete definition

To add a request property

1. In the Manager, select the **IT Shop > Basic configuration data > Request properties** category.
2. Click in the result list.

3. Enter the name and a description for the request property.
4. Enable the **Obsolete definition** option.

   After saving, the option cannot be changed again.
5. Save the request property.
6. Select the **Parameter** tab.
7. Click **Add**.
8. Edit the request parameter's main data.
9. To add another request parameter, click **Add**.
10. Save the changes.

Editing request properties

To edit a request property

1. In the Manager, select the **IT Shop > Basic configuration data > Request properties** category.
2. Select the request property in the result list.
3. Select the **Change main data** task.
4. Edit the request property's main data.
5. Save the changes.
6. Recompile the database if the scripts for calculating values have been changed in the parameter settings.

Detailed information about this topic

- Request property and request parameter settings on page 41
- Copy request properties on page 47

Related topics

- Main data for service categories on page 36
- General main data for service items on page 23

Request property and request parameter settings

Enter the following main data for a request property.

Table 9: Request property main data

Property	Description
Request	Name of the request property.

Property	Description
property	
Description	Exact description of the request properties.
Obsolete definition	Specifies whether an obsolete definition is used for the request parameter. This information cannot be changed after a new request property has been saved.

Settings for request parameters with the current definition

Request parameters with the current definition are saved in the `DialogParameter` table. All a request property's parameters are grouped together internally as a parameter set (`DialogParameterSet`). The parameter settings defined in the Manager are saved as default parameters. During the request, fixed parameter values can be entered in the Web Portal. These values are saved per request in parameter subsets. If the request has not entered a value, the parameter value from the default parameter set is used.

IMPORTANT: If the parameter settings in the default parameter set are changed and, as long as the requester has not entered their own values, the changes are passed on to all the requests in the shopping cart that use this parameter set.

NOTE: The **`Inherited`** value can be selected for various parameter settings. This does not affect request parameters. The parameter settings' default values apply that are shown next to the input fields.

There are three tabs for editing the parameter settings, the value definition, and scripts for calculating the values. The actual parameter values are shown next to the fields and menus.

General tab

Table 10: General parameter settings

Property	Description
Parameter name	Parameter name.
Parameter type	Type of parameter. Permitted values are: • **`Fixed`**: Fixed parameter values are used. On the **Value definition** tab, enter the parameter value. • **`User prompt`**: The user must select a parameter value in the user prompt during the request. • **`Calculation`**: The parameter value is calculated during the request. On the **Value calculation** tab, enter the table column and the condition for calculating the value. Other settings are shown or hidden depending on the type.
Display name	User friendly name for the parameter. To display language dependent display names, translate the given text with the button.

Property	Description
Description	Text field for additional explanation.Translate the given text with the button.
Sort order	Position of the parameter in the request property view in the Web Portal. Parameters with a low sequence values are display at the top.
Mandatory parameter	Specifies whether this is a mandatory parameter. This parameter must have a value in it in order to make the request.
Viewable	Specifies whether the parameter is shown in the request in the Web Portal. The parameter value displayed here is transferred to the subparameter set for this request.
Overridable	Specifies whether the parameter value can be overwritten during the request.

Value definition tab

Table 11: Value definition

Property	Description
Data type	Parameter data type.
Date add-on	Additional information about calculating date data and time data for displaying in the user interface. The value can be edited if the **Date** data type is selected. Permitted values are: • **Date and time**: Date-time values can be entered and read out. In One Identity Manager tools, the data saved in UTC is automatically converted to local time. The user, therefore, sees all the values in local time. • **Date only**: Only the date can be entered and displayed. Time slices are ignored and there is not time zone conversion. • **End of day**: Only the date is relevant for this format. The time slice of **23:59:59** local time is automatically assumed unless a time (not equal to **00:00:00**) is explicitly passed down. A user or service that writes a time entry like this, defines the end of the day according to its time zone. • **UTC date and time**: Date-time values can be entered and read out. In the One Identity Manager tools, there is no conversion from UTC to local time or vice versa.
Value range	Specifies whether the report parameter value has to be within a given range. If **Yes**, additional fields appear.
Multivalue	Specifies whether the parameter accepts multiple values. If **Yes**, users can select multiple value from a list.

Property	Description
Multiline	Specifies whether the parameter contents can have multiple lines. If **Yes**, line breaks are permitted.
Data source	Type of data source. Permitted values are: • **None**: The user can give any value. • **Table**: The user selects a value from a specified table column. • **List of permitted values**: The user selects a value from a predefined list. You may require additional data depending on the data source.
Table column (query)	Additional data for the data source **Table**. Table column for selecting the parameter value. The user can select a value from this table column. If the parameter is multi-value, you can select several values from this column as well.
Display pattern	Additional data for the data source **Table**. Display pattern for table elements in lists in `%column%` notation. The `??` operator is permitted. This means, when one column's value is empty, another column's value is displayed. Example: `%column1??column2??column3%`
Type of display	Specifies how data for the value query is displayed. For example, data from a hierarchical table can be displayed either hierarchically or in a list without a hierarchy. Permitted values are: • **Hierarchical**: (Default) The data is displayed hierarchically. • **List**: The data is displayed in a list. • **Inherited**: The setting is inherited.

Condition (query)	Additional data for the data source **Table**.
	Limiting condition (Where clause) for selecting the parameter value using a table column. The user can select a value from the result set. If the parameter is multi-value, you can select several values from this result set as well.
	You can reference other parameters in the condition using the following syntax:
	`$PC(<Parametername>)$`
	Example:
	`FullPath like CONCAT('%',$PC(P1)$,'%')`
	`where P1 is the name of the referenced parameter.`

List of	Additional data for the data source **List of permitted values**.

Property	Description
permitted values	List of values permitted in this parameter in the `value=display name` notation. If an = is no given, the entry counts as both value and display name. Example: `1=internal 2=external` To display language dependent display names, translate each display name using the button.
Overwrite empty value	Specifies whether an empty parameter value overwrites the default value. If this option is disabled, the default value is overwritten if a parameter value is not given.
Parameter value	Parameter value If a value range is given, the **Parameter value (from)** and the **Parameter value (to)** are displayed.
Example value	Example of the parameter. If a value range is given, the **Example value (from)** and the **Example value (to)** are displayed.
Default value	Default value of the parameter. This is used if the user does not specify a parameter value and the **Overwrite empty value** option is not set. If a value range is given, the **Default value (from)** and the **Default value (to)** are displayed.

Value calculation tab

Table 12: Scripts for calculating values

Property	Description
Table column (calc.)	Additional input for `Calculated` parameter type. Table column for selecting the parameter value. The parameter value is calculated during the request.
Condition (calc.)	Additional input for `Calculated` parameter type. Limiting condition (where clause) for selecting the value through a table column. The parameter value is calculated during the request. If the parameter is multivalue as well, several values may be found. If a condition is not given and the parameter is not multivalue, the first value is used that is determined by the table column. If the parameter is multivalue and a condition is not given, all determined values are used.

Valuation script	Script in VB.Net syntax, which can be used to change the value when the parameter is called. This does not change the saved value.
	Example:
	`Value = DateTime.UtcNow`
	`Value = 42`

Property	Description
	`Value = DbVal.ConvertTo(Of String)(Value).ToUpperInvariant()`

Validation script	Script in VB.Net syntax for checking permitted values of parameters. Write a script that checks user input and sets a value if necessary.
	Example:
	Changing a value during the assignment
	`Value = DbVal.ConvertTo(Of String)(Value).ToUpperInvariant()`
	Test a value
	`Dim str = Convert.ToString(value)`
	`If str.Contains("1") Then`
	`Throw New ViException(#LD( "Parameter1 must not contain {0}",str)#,ExceptionRelevance.EndUser)`
	`End If`

Data dependencies script	Script in VB.Net syntax to adjust the parameter settings depending on the data. The script is run during initialization and when values are changed. For example, the script can be used to dynamically determine whether a parameter is read-only or mandatory. Example: Parameter **P2** should be a mandatory parameter if parameter **P1** has the value **1**. The following script must be stored with the **P1** parameter. `ParameterSet("P2").IsMandatory = (Value IsNot Nothing AndAlso Value.ToString() = "1")`

TIP: When entering the scripts, you can use supporting functions such as auto-complete or code snippets. For more information about support for scripting in the Script Editor and also general information about using scripts in One Identity Manager, see *One Identity Manager Configuration Guide*.

Request parameter main data for obsolete definition

Request parameters with an obsolete definition are saved in the `AccProductParameter` table. In a request parameter's main data, you specify the column in the `ShoppingCartItem` table where request parameter is saved during the request. If the selected column is a foreign key column, the requester can select from list of permitted values from in the Web Portal. The values can be limited by a condition. If the selected column allows free text, the requester must enter the request property as text in the Web Portal.

NOTE: If you want to use custom column to store request properties, add identical columns to the tables `ShoppingCartItem` and `PersonWantsOrg`.

Table 13: Request property main data

Property	Description
Column	Column of the `ShoppingCartItem` table where the parameter value is saved

Property	Description
	during the request.
Display value	User friendly name for the parameter. To display language dependent display values, translate the given text with the button.
Sort order	Sort order in which to display the request properties in the Web Portal.
Mandatory parameter	Specifies whether this is a mandatory parameter. This parameter must have a value in it in order to make the request.
Read-only	Specifies whether the parameter should only be viewable in the Web Portal and not editable.
Editable for approver	Specifies whether the parameter can also edited by approvers. If this option is set, the parameter value that was entered by the requester can be changed by the approver. If this option is not set, only the requester can enter a value.
Condition	Condition limiting a foreign key value list.

Related topics

- Entering product-specific request properties on page 40

Copy request properties

To reuse existing definitions of request parameters, you can copy the request properties.

To copy a request property

1. In the Manager, select the **IT Shop > Basic configuration data > Request properties** category.
2. Select the request property in the result list.
3. Select the **Create copy** task.
4. Enter a name for the new request property and click **OK**.

   This creates a request property with the given name. You can now edit the request properties of this request property.

Related topics

- Request property and request parameter settings on page 41
- Entering product-specific request properties on page 40

Displaying the request properties overview

On the overview form, you see, at a glance, the most important information about a request property.

To obtain an overview of a request property

1. In the Manager, select the **IT Shop > Basic configuration data > Request properties** category.
2. Select the request property in the result list.
3. Select the **Request properties overview** task.

Related topics

- Request property and request parameter settings on page 41

Products for requests with time restrictions

Customers retain their requested products until they cancel 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.

To enter a validity period for products

To specify a validity period for a product request

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the service item in the result list.
3. Select the **Change main data** task.
4. Enter in the **Validity period (max. # days)** field the time period within which the product can be requested.

   INFORMATION: This value has no effect on requests for multi-request resources (`QERReuse`).
5. Save the changes.

One Identity Manager calculates the date that the product is automatically canceled from the current data and validity period at the time of request and approval.

Product request on customer or product relocation

If a customer requests a product from a shop or shopping center and then changes to another at a later date, you must decide how the existing request should be handled. The same applies if a product is moved to another shelf after the request. In both cases, One Identity Manager checks whether the request recipient and the product belong to the same new shop after relocating.

Table 14: Effects of relocating

Request recipient and product	Effect on approved requests	Effect on pending requests
Are in different shops	The request is canceled. The assignment is removed.	The request is canceled.
Are in the same shop	Behavior is defined by **Retain service item assignment on relocation** in the service item.	

Closed requests are not changed.

If the request recipient and the product belong to the same shop after relocating, the **Retain service item assignment on relocation** option controls whether the request is canceled or retained.

Table 15: Effect of the "retain service item assignment on relocation" option

Option Value	Effect on approved requests	Effect on pending requests
Not set	The request is canceled. The assignment is removed.	The request is canceled.
Enabled	The request remains intact. Shelf and shop are updated in the request procedure. Assignment of requested company resources remains intact.	The request remains intact. Shelf and shop are updated in the request procedure. Approvals already granted, are reset. The request runs through the approval process implemented in the new shop.

NOTE: The request is realized in the shop in which the request recipient is customer and that contains the requested product. If several shelves or shops are found to which the condition applies, One Identity Manager selects one of the shelves or shop, respectively, to relocate.

The complete approval sequence is shown in the approval history.

To obtain a product's requests on relocation

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the service item in the result list.
3. Select the **Change main data** task.
4. Set the **Retain service item assignment on relocation** option.
5. Save the changes.

Related topics

- Request statuses on page 273
- Restructuring the IT Shop on page 230

Non-requestable products

Products that have already been requested but can only be requested for a limited period, can be specially labeled for it. Existing request for the product remain intact. However, no new requests may be made for the product.

To label a product as not requestable

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.
2. Select the product's service item in the result list.
3. Select the **Change main data** task.
4. Set **Not available**.
5. Save the changes.

Entering terms of use for service items

Terms of use that explain conditions of use for a product can be stored for individual service items (for example, software license conditions). When someone requests this product, the requester, and request recipient must accept the terms of use before the request can be finalized.

To add or edit terms of use

1. In the Manager, select the **IT Shop > Terms of use** category.
2. In the result list, select a terms of use and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the terms of use main data.
   - **Terms of use**: Terms of use identifier.
   - **Description**: Text field for additional explanation.
   - **Content**: Complete text of the terms of use.

     Alternatively, the terms of use can be attached as a PDF file.
   - **Multifactor authentication required**: Specifies whether multifactor authentication via the configured provider is required by requests to accept the terms of use.
4. Save the changes.
5. Assign the terms of use to service items.

In order for the request recipient to accept the terms of use, the request must be assigned to the request recipient in the approval process. Set an approval workflow for such requests that contain a BR approval step and enable the **No automatic approval** option for this approval step. One Identity Manager provides a default approval workflow and a **Terms of Use acknowledgment for third-party orders (sample)** default approval policy that you can use for this.

Related topics

- Approving requests with terms of use on page 163
- General main data for service items on page 23
- Assigning files to terms of use on page 51

Assigning files to terms of use

The full-text of the terms of use is provided as a PDF file in different languages. These PDF files are loaded into the One Identity Manager database and can be displayed when requesting and approving a product or for attestors in the Web Portal. The PDF file matching the user's login language is offered.

To load PDF files for the terms of use into the database

1. In the Manager, select the **IT Shop > Terms of use** category.
2. Select the terms of use in the result list.
3. Select the **Assign files** task.

4. Click **Add**.
5. In the **Language** drop-down, select the language you want the PDF file to be in.

   All the languages that are configured as login languages in the One Identity Manager tools are provided.
6. Next to the **File** field, click .
7. In the **Open** dialog, select the PDF file and click **Open**.
8. To load other PDF files, click **Add** and repeat the step.
9. Save the changes.

To delete a PDF file of a terms of use from the database

1. In the Manager, select the **IT Shop > Terms of use** category.
2. Select the terms of use in the result list.
3. Select the **Assign files** task.
4. In the list, select a file and click **Remove**.
5. Save the changes.

Related topics

- Entering terms of use for service items on page 50

Displaying the terms of use overview

You can display the most important information about a tag on the overview form.

To obtain an overview of the terms of use

1. In the Manager, select the **IT Shop > Terms of use** category.
2. Select the terms of use in the result list.
3. Select the **Terms of use overview** task.

Related topics

- Entering terms of use for service items on page 50

Entering tags

Product owners are able to add tags to their products. These tags can be used as search criteria by requests in the Web Portal. There are two ways of adding tags.

To add or edit a tag

1. In the Manager, select the **IT Shop > Basic configuration data > Tags** category.
2. In the result list, select a tag and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the tag data.
4. Save the changes.

Enter the following data for a tag.

Table 16: General main data of a tag

Property	Meaning
Tag	Tag.
Description	Tag description.
Comment	Text field for additional explanation.
Parent tag	Tags can be organized hierarchically. Assign a parent tag to do this.

To add a tag directly to a product

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the service item in the result list.
3. Select the **Assign tag** task.
4. Select the **Create tag** task.
5. Enter the tag and a description for it.
6. Click **Ok** to save the tag.

   The new tag is shown on the assignment form.
7. Double-click on the tag to assign it to the selected service item.
8. Save the changes.

Assigning service items to tags

Assign service items to the tags so that you can use the tags as search terms in the Web Portal. The Web Portal finds all the requestable service items assigned to a tag.

To assign a tag to a service item

1. In the Manager, select the **IT Shop > Basic configuration data > Tags** category.
2. Select a tag in the result list.
3. Select the **Assign service items** task.

   In the **Add assignments** pane, assign service items.

   TIP: In the **Remove assignments** pane, you can remove service item assignments.

   To remove an assignment

   - Select the service item and double-click ✓.
4. Save the changes.

Displaying the tags overview

The overview form contains the most important information about a tag.

To get an overview of a tag

1. In the Manager, select the **IT Shop > Basic configuration data > Tags** category.
2. Select a tag in the result list.
3. Select the **Tag overview** task.

Assigning and removing products

Once you have prepared the product to be requested, assign it to a shelf or a shelf template. A shelf has several tasks available for assigning and removing products.

NOTE: The tasks are only displayed if the **Assignments permitted** and **Direct assignment permitted** options are enabled for the **IT Shop structure** or **IT Shop template** role classes.

Table 17: Tasks for assigning and removing requestable products

Products	Task
Software	Assign software
Resources	Assign resource
Multi-request resources	Assign resource
Multi requestable/unsubscribable resources	Assign resource

Products	Task
System roles	Assign system roles
Groups and system entitlements from custom target systems	Assign system entitlements of custom target systems
Active Directory groups	Active Directory Assign groups
Microsoft Entra ID permissions	Microsoft Entra ID Assign groups
	Microsoft Entra ID Assign administrator roles
	Microsoft Entra ID assign subscriptions
	Assigning disabled Microsoft Entra ID service plans
SharePoint permissions	SharePoint Assign groups
	Assign SharePoint roles
LDAP groups	LDAP Assign groups
HCL Domino groups	Notes Assign groups
SAP R/3 permissions	Assign BI analysis authorizations
	SAP Assign groups
	Assign SAP profiles
	Assign SAP roles
	Assigning structural profiles
E-Business Suite permissions	Assign E-Business Suite authorizations
Exchange Online permissions	Assign Exchange Online mail-enabled distribution groups
	Microsoft 365 Assign groups
Privileged Account Management permissions	Assign PAM user groups
SharePoint Online permissions	SharePoint Online Assign groups
	Assign SharePoint Online roles
Google Workspace permissions	Google Workspace Assign groups
	Google Workspace Assign products and SKUs
Unix groups	Unix Assign groups
Cloud groups and system entitlements	Assign cloud groups and system entitlements

Products	Task
Subscribable reports	Assign subscribable reports
Assignment resources	Assign resource
Account definitions	assign account definition

Detailed information about this topic

- Role classes for the IT Shop on page 211

Assigning products to shelves

There are different tasks available for assigning a single product from a shelf. The following example based on a resource shows you how to assign individual products.

To assign a resource to the Identity Lifecycle shelf as a product

1. In the Manager, select the **IT Shop > IT Shop > Identity & Access Lifecycle > Shelf: Identity Lifecycle** category.
2. Select the **Assign resources** task.
3. Select the **Resources** tab and, in the **Add assignments** section, select the resources with a double-click.
4. Save the changes.

Products are automatically assigned to shelves at the same time, if:

- Groups are automatically added to the IT Shop
- Rule templates are used to set up the IT Shop

Use the DBQueue Processor inheritance mechanism and subsequent post-processing to create a separate product node for each assigned product within the shelf. These product nodes are displayed with the name of the product's service item. If products are added in bulk to the IT Shop by automatic processes, you can specify how many product nodes are created in one DBQueue Processor run in the **QER | ITShop | LimitOfNodeCheck** configuration parameter. Once this number has been exceeded, the task is closed and queued again in the DBQueue for generating the rest of the product nodes. By default, 500 objects are processed in one run.

Related topics

- Adding system entitlements automatically to the IT Shop on page 81
- Templates for automatically filling the IT Shop on page 232

Removing products from shelves

There are different tasks available for removing a product from a shelf. In the following section, we take the example of a resource to show how to remove a product.

To remove a resource from the Identity Lifecycle shelf

1. In the Manager, select the **IT Shop > IT Shop > Identity & Access Lifecycle > Shelf: Identity Lifecycle** category.
2. Select the **Assign resources** task.
3. Select the **Resources** tab and, in the **Remove assignments** section, double-click the resources.
4. Save the changes.

When you remove a product from a shelf, pending requests for the product are closed and approved requests are unsubscribed.

To remove a product from all shelves

- Select the **Remove from all shelves** task.

  You will find the task on the main data form of the respective product, for example, a resource.

The task immediately removes product assignments to manually configured shelves and shelf templates. Then, the DBQueue Processor removes product assignments to shelves, based on a template definition. All assignments are unsubscribed if the product is part of an assignment request.

Information on bulk processing

If products are added in bulk to the IT Shop by automatic processes, you can specify how many product nodes are created in one DBQueue Processor run in the **QER | ITShop | LimitOfNodeCheck** configuration parameter. Once this number has been exceeded, the task is closed and queued again in the DBQueue for generating the rest of the product nodes. By default, 500 objects are processed in one run. The number of requests submitted in bulk can be considerably larger than other processes.

Set a lower value if performance issues arise when running the `QER-K-OrgAutoChild` process task.

Moving products to another shelf

A product can be moved to another shelf. If the shelf is in another shop, the system checks whether the request recipient is also a customer in the new shop.

NOTE: Standard products cannot be moved.

To move a product to another shelf

1. In the Manager, select the **IT Shop > IT Shop > <shop> > Shelf: <shelf>** or the **IT Shop > IT Shop > <shopping center> > <shop> > Shelf: <shelf>** category.
2. Select an object in the result list.
3. Select the **Move to another shelf** task.
4. Select the new shelf.
5. Click **OK**.

To move multiple products to another shelf

1. In the Manager, select the **IT Shop > IT Shop > <shop>** category or the **IT Shop > IT Shop > <shopping center> > <shop>** category.
2. Select the shelf in the result list.
3. Select the **Move products to another shelf** task.
4. Select the shelf to move the products to.
5. Select which products to move.
6. Click **OK**.

Detailed information about this topic

- Product request on customer or product relocation on page 49
- Restructuring the IT Shop on page 230

Replacing products

A product can be replaced by another product at a specified time. All identities who have requested this product are notified by an email telling them to request a replacement product.

To replace a product with another one

1. In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > <service category>** category.

   - OR -

   In the Manager, select the **IT Shop > Service catalog > Hierarchical by service categories > Singles** category.
2. Select the product's service item to replace in the result list.
3. Select the **Change product** task.
4. Enter the following data:

- **Expiry date**: Date on which the product is replaced by a different product.
- **Alternative product**: Service item that can be requested instead.

5. Click **OK**.

Related topics

- Product change notifications on page 190

Preparing the IT Shop for multi-factor authentication

You can use multi-factor authentication for specific security-critical resource requests, which requires every approver for the request approval to authenticate themselves again. Define which products require this authentication in your service items.

One Identity Manager uses OneLogin for multi-factor authentication. Usable authentication modes are determined through the OneLogin user accounts linked to the identities.

Prerequisites

In OneLogin:

- At least one authentication method is configured on all user accounts that are going to use multi-factor authentication.

In One Identity Manager:

- The OneLogin Module is installed.
- Synchronization with a OneLogin domain is set up and has been run at least once.
- Identities linked to OneLogin user accounts.
- The API Server and the web application are configured as required.

For more information about setting up multi-factor authentication, see the *One Identity Manager Authorization and Authentication Guide*.

To use multi-factor authentication in the IT Shop

- In the Manager, create service items for the product that can only be requested with multi-factor authentication.
  - Enable the **Approval by multi-factor authentication** option.

Once the **Approval by multi-factor authentication** option is enabled on a service item, additional authentication is requested in each approval step of the approval process. Approvers can select any one of the authentication methods assigned to their OneLogin user accounts.

IMPORTANT: An approval cannot be sent by email if multi-factor authentication is configured for the requested product. Approval mails for such requests produce an error message.

For more information about requesting products requiring multi-factor authentication and about canceling products, see the *One Identity Manager Web Portal User Guide*.

Related topics

- General main data for service items on page 23
- Approval by mail on page 191

Assignment requests

You can also use One Identity Manager to request hierarchical roles, like departments, or business roles, through the IT Shop and assign them to identities, devices, and workdesks. This allows any number of assignments to be made through IT Shop requests. The advantage of this method is that any assignments can be authorized using an approval process. Assignment renewals and assignment recall are also subject to an approval process in the same way. The request history makes it possible to follow which assignments were requested, renewed, or canceled, why, when, and by whom.

The managers of business roles, organizations, and system roles can make assignments requests for their roles.

In the Web Portal, managers of business roles, organizations, and system roles can see assignments requests for roles under their supervision. Use the **QER | ITShop | ShowClosedAssignmentOrders** configuration parameter to specify whether all assignment requests are displayed or only open ones. By default, pending as well as closed assignment requests are displayed.

To only display a manager's pending assignment requests in the Web Portal

- Disable the **QER | ITShop| ShowClosedAssignmentOrders** configuration parameter in the Designer.

Standard products for assignment requests

You require special resources, so-called assignment resources, for assignment requests. Assignment resources are linked to service items and can thus be made available as products in the IT Shop.

One Identity Manager provides standard products for assignment requests. These are used to:

- Request membership in business roles or organizations for which the logged-in One Identity Manager user is responsible.
- Request system entitlement assignments or other company resources to system roles, business roles, or organizations for which the logged in One Identity Manager user is responsible.

Table 18: Standard products for assignment requests

Assignment resource	Service item	Shop | Shelf	Request
Members in roles	Members in roles	Identity & Access Lifecycle | Identity Lifecycle	Memberships in business roles, application roles, and organizations
Role entitlement assignments	Role entitlement assignments		Assignment of company resources to business roles and organizations
System role assignments	System role assignments		Assignment of company resources to system roles

In the default installation, all active One Identity Manager database identities are customers of the **Identity & Access Lifecycle** shop. This allows all active identities to request memberships and assignments. The assignment requests are automatically approved by self-service.

You can add standard products for assignment requests to your own IT Shop.

Assignments can only be requested from and for customers of this shop. This means, the manager of the hierarchical roles as well as the identities that are also members of these roles, must be customers in the shop.

TIP: Assignment requests can also be made for custom assignment tables (many-to-many tables), if they have an `XOrigin` column. The properties for this column must correspond to the column definition for `XOrigin` columns in the One Identity Manager data model.

Example for an assignment request

Jo User1 is the project X project leader. A business role (Project X) is added in the Manager to ensure that all the project staff obtain the necessary entitlements. Jo User1 is assigned as manager of this business role. All project staff have a user account in the Active Directory domain P.

Jo User1 can request memberships in the Project X business role in the Web Portal because they are a manager. Jo User1 requests memberships for themselves and all project staff.

Furthermore, Jo User1 wants all project staff to obtain their entitlements in Active Directory through the Project X AD permissions Active Directory group. To this, they request Project X AD permissions in the Web Portal for the Project X business role.

The user accounts of all project staff become members in the Project X AD permissions Active Directory group through internal inheritance processes.

For more information, see the *One Identity Manager Web Portal User Guide*.

Related topics

- Examples of request results on page 275

Requesting memberships in business roles

NOTE: This function is only available if the Business Roles Module is installed.

You have the option to limit assignment requests to single business roles. To do this, an assignment resource is created for a fixed requestable business role. The business role is automatically part of the request in an assignment resource request. If the request has been approved, the requester becomes a member of the application role.

Each requestable business role of this kind can have its own approval process defined. The service items connected with the assignment resources are assigned separate approval policies in order to do this.

To limit assignment requests to single business roles

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Create assignment resource** task.

   This starts a wizard that takes you through the steps for adding an assignment resource.

   a. Enter a description and allocate a resource type.

      This creates a new assignment resource with the following custom properties:

      - **Table**: Org
      - **Object**: Full name of business role

   b. Enter the service item properties to allocate to the assignment resource.

      - Assign a service category so that the assignment resource in the Web Portal can be ordered using the service category.

   A new service item is created and linked to the assignment resource.

4. Assign the assignment resource to an IT Shop shelf as a product.
5. Assign an approval policy to the shelf or the assignment resource's service item.

Assignment resource and service item main data can be processed later on if required.

The assignment resource can be requested in the Web Portal like any other company resource. After the request has been successfully assigned, the identity for whom it was requested becomes a member of the associated business role through internal inheritance processes. For more information about requesting assignment resources, see the *One Identity Manager Web Portal User Guide*.

The assignment resource cannot be used to request the assignment of company resources to this business role. Instead, use the **Role entitlement assignment** default assignment resource.

Related topics

- Adding assignment resources to the IT Shop on page 70
- General main data for service items on page 23
- Assigning requestable products to shelves on page 222
- Setting up assignment resources on page 67
- Entering service items on page 22

Requesting memberships in application roles

You have the option to limit assignment requests to single business roles. To do this, an assignment resource is created for a fixed requestable application role. The application role then automatically becomes part of the assignment resource request. If the request is approved, the requester becomes a member of the application role.

Each requestable application role of this kind can have its own approval process defined. The service items connected with the assignment resources are assigned separate approval policies in order to do this.

To limit assignment requests to single application roles

1. In the Manager, select an application role in the **One Identity Manager Administration** category.
2. Select the **Create assignment resource** task.

   This starts a wizard that takes you through the steps for adding an assignment resource.

   a. Enter a description and allocate a resource type.

      This creates a new assignment resource with the following custom properties:

- **Table**: AERole
- **Object**: Full name of application role

b. Enter the service item properties to allocate to the assignment resource.
   - Assign a service category so that the assignment resource in the Web Portal can be ordered using the service category.

   A new service item is created and linked to the assignment resource.

3. Assign the assignment resource to an IT Shop shelf as a product.
4. Assign an approval policy to the shelf or the assignment resource's service item.

Assignment resource and service item main data can be processed later on if required.

The assignment resource can be requested in the Web Portal like any other company resource. After the request has been successfully assigned, the identity for whom it was requested becomes a member of the associated application role through internal inheritance processes. For more information about requesting assignment resources, see the *One Identity Manager Web Portal User Guide*.

Related topics

- Adding assignment resources to the IT Shop on page 70
- General main data for service items on page 23
- Assigning requestable products to shelves on page 222
- Setting up assignment resources on page 67
- Entering service items on page 22

Customizing assignment requests

Assignment requests with standard products are automatically approved through self-service. If assignment requests are going to be approved by an approval supervisor, assign a suitable approval policy to the default assignment resource. This means that assignment requests also go through the defined approval process.

To approve assignment requests through an approver

- Assign separate approval policies to the default assignment resources service items.

  - OR -

- Assign any approval policy to the **Identity Lifecycle** shelf.

Sometimes assignment requests should be subject to various approval processes depending on the object requested. For example, the department manager approves memberships in department A, but memberships in department Z are approved by the managers of the identities. You can define assignment resources to do this. You can assign these assignment resources to any shelf in your IT Shop.

To configure customized assignment requests

1. Create a new assignment resource.
    a. In the Manager, select the **Entitlements > Assignment resources for IT Shop** category.
    b. Click in the result list.
    c. Select the **Change main data** task.
    d. Edit the following master data:
        - **Assignment resource**: Name of the assignment resource.
        - **Service item**: Assign a new service item.
        - **Table**: Table used for the assignment, such as `Department`.
        - **Object**: Fixed hierarchical role to which the identities are assigned (`Department A` for example).
    e. Save the changes.
2. Assign the assignment resource to an IT Shop shelf as a product.
    a. Select the **Add to IT Shop** task.
    b. In the **Add assignments** pane, assign a shelf.
    c. Save the changes.
3. Assign an approval policy to the shelf or the assignment resource's service item.

The `VI_GetAccproductAssignmentMember` script uses the object key of the requested assignment (`ObjectKeyAssignment`) to determine the assignment resource and service item that apply to the request. In the Designer, modify this script according to your requirements.

Detailed information about this topic

- General main data for assignment resources on page 68
- Adding assignment resources to the IT Shop on page 70
- General main data for service items on page 23
- Assigning requestable products to shelves on page 222
- Assigning approval policies on page 222

Related topics

- Approval processes for IT Shop requests on page 85

Canceling requests

Assignments, like all other products, can be canceled through Web Portal or requested for a limited time period. These requests are automatically canceled when the validity period

expires. For more information, see the *One Identity Manager Web Portal User Guide*.

Detailed information about this topic

- Requests with limited validity period on page 172

Removing customers from a shop

If a customer has requested assignment through a shop and later they are removed from the shop, then the assignment request is closed and the assignment is revoked. In this case, however, assignments to roles should be retained if required.

To prevent the assignment from being revoked

1. In the Designer, set the **QER | ITShop | ReplaceAssignmentRequestOnLeaveCU** configuration parameter.
2. (Optional) Enable the **QER | ITShop | ReplaceAssignmentRequestOnLeaveCU | UID_PersonFallback** configuration parameter in the Designer.
    - In the **Value** field, enter the `UID_Person` of the identity that should be used as the fallback if no other request recipient can be found.

      This identity must be a customer in all shops in which which assignments can be requested.
3. Save the changes.
4. In the Manager, select the **Entitlements > Assignment resources for IT Shop** category.
5. In the result list, select an assignment resource and select the **Change main data** task.
6. Set the **Keeps requested assignment resource** option.
7. Save the changes.

This option is enabled by default for the **Role entitlement assignment** default assignment resource. These configuration parameters are disabled by default.

If this option is enabled and the request recipient is removed from the customer node, then the request is updated according to the following rules:

1. If the service item
    - Has the **Retain service item assignment on relocation** option set
    - The request recipient and service item are available in another shop

   The assignment request is transferred into this shop. The request recipient remains the same.
2. If by doing this the request recipient does not remain the same, then a new request recipient is determined.

a. The manager of the business role or organization that has been requested (`PersonWantsOrg.ObjectKeyOrgUsedInAssign`).

b. A member of the business role or organization that has been requested.

c. A member of the chief approval team.

d. The identity given in the **QER | ITShop | ReplaceAssignmentRequestOnLeaveCU | UID_PersonFallback** configuration parameter.

These rules are applied in the order given. The identity that is found must be a customer in the shop.

If no authorized approver can be found or the **QER | ITShop | ReplaceAssignmentRequestOnLeaveCU** configuration parameter is disabled, then the assignment request is converted into a direct assignment. If direct assignment for the assigned product is not permitted to the requested business role or organization, the request is canceled and the assignment is removed.

NOTE: This option does not influence membership requests in roles or delegation.

Membership assignments are not removed, if the requester is removed from the customer node. They are removed when the recipient of the assignment request is deleted from the customer node.

Delegation ends when the delegate is deleted from the customer node.

Related topics

- General main data for assignment resources on page 68
- Relocating a customer or product to another shop on page 176

Setting up assignment resources

To edit an assignment resource

1. In the Manager, select the **Entitlements > Assignment resources for IT Shop** category.
2. In the result list, select an assignment resource and run the **Change main data** task.
3. Edit the assignment resource's main data.
4. Save the changes.

To create an assignment resource

1. In the Manager, select the **Entitlements > Assignment resources for IT Shop** category.
2. Click in the result list.

3. Edit the assignment resource's main data.
4. Save the changes.

Detailed information about this topic

- General main data for assignment resources on page 68

General main data for assignment resources

Enter the following main data of an assignment resource.

Table 19: Main data for an assignment resource

Property	Description
Assignment resource	Name for the assignment resource.
Resource type	Resource type for grouping assignment resources. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.
IT Shop	Specifies whether the assignment resource can be requested through the IT Shop. The assignment resource can be requested through the Web Portal and allocated by defined approval processes. This option cannot be disabled.
Only for use in IT Shop	Specifies whether the assignment resource can be requested through the IT Shop. The assignment resource can be requested through the Web Portal and allocated by defined approval processes. The assignment resource cannot be directly assigned to roles outside the IT Shop. This option cannot be disabled.
Service item	Service item through which you can request the assignment resource in the IT Shop. Assign an existing service item or add a new one.
Table	Table where the assignment should be made. Assignment requests can be limited to a specific hierarchical role. Choose the table from which the role should be selected.
Object	Specific hierarchical role that identities can request. Only one assignment resource can be created per role.
Description	Text field for additional explanation.
Risk index	Value for evaluating the risk of assigning the assignment resource

Property	Description
	to identities. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Requested assignments remain intact.	If this option is set, requested role assignments are converted into direct assignments if the request recipient is removed from the customer node of the associate shops. The option can only be edited as long as there is a request has not been assigned with this assignment resource.
Assignment to system roles	Specifies whether the assignment resource is used for requesting assignments to system roles. Disable this option if requesting memberships in hierarchical role or hierarchical role assignments.
Spare field no. 01 ... Spare field no. 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Detailed information about this topic

- Entering service items on page 22
- Removing customers from a shop on page 66

Related topics

- Requesting memberships in business roles on page 62
- Requesting memberships in application roles on page 63

Default assignment resources

One Identity Manager provides standard products for assignment requests. These are assigned to the **Identity & Access Lifecycle** shop as default assignment resources.

To edit default assignment resources

- In the Manager, select the **Entitlements > Assignment resource for IT Shop > Predefined** category.

Displaying assignment resource overviews

Use this task to obtain an overview of the most important information about an assignment resource. For this, you need to take into account the affiliation of the assignment resource to IT Shop structures.

To obtain an overview of a service item

1. In the Manager, select the **Entitlements > Assignment resources for IT Shop** category.
2. Select the assignment resource in the result list.
3. Select the **Assignment resource overview** task.

Adding assignment resources to the IT Shop

An assignment resource can be requested by shop customers when it is assigned to an IT Shop shelf.

To add a resource assignment to the IT Shop

1. In the Manager, select the **Entitlements > Assignment resources for IT Shop** category.
2. Select the assignment resource in the result list.
3. Select the **Add to IT Shop** task.
4. To assign the assignment resource to shelves, select the **IT Shop shelves** tab and, in the **Add assignments** section, select the shelves with a double-click.
5. To assign the assignment resource to IT Shop templates, select the **IT Shop templates** tab and, in the **Add assignments** section, select the template with a double-click.
6. Save the changes.

Removing assignment resources from the IT Shop

To remove an assignment resource from all IT Shop shelves.

1. In the Manager, select the **Entitlements > Assignment resources for IT Shop** category.
2. Select the assignment resource in the result list.
3. Select the **Add to IT Shop** task.
4. To remove the assignment resource from the shelves, select the **IT Shop shelves** tab and, in the **Remove assignments** section, double-click the shelves.

5. To remove the assignment resource from the IT Shop templates, select the **IT Shop templates** tab and, in the **Remove assignments** section, double-click the shelves.
6. Save the changes.

To remove an assignment resource from all IT Shop shelves.

1. In the Manager, select the **Entitlements > Assignment resources for IT Shop** category.
2. Select the assignment resource in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   The One Identity Manager Service removes the assignment resource from all shelves. All assignment requests with this assignment resource are canceled in the process.

Delegations

Role assignment and responsibilities can be temporarily delegated to others. Thereby, a distinction is made between single delegations and deputizing.

- **Deputize**: Delegate all your responsibilities for a defined area to a deputy. The following areas can be selected:
  - Approval authorization for requests

    Once an identity is determined as the approver for requests, their deputy is added as an additional approver.
  - Exception approval requests violate the rules

    Once an identity is determined as the exception approver for requests, their deputy is added as an additional exception approver.
  - Approval authorization in attestation cases

    Once an identity is determined as the attestor, their deputy is added as an additional attestor.
  - Manager of identities

    The deputy of an identity's manager can also approve managerial tasks. For example, a deputy can initiate requests for employees.
  - Manager of all roles of a role class

    The deputy of a hierarchical roles manager can also approve all managerial tasks. For example, a deputy can initiate assignment requests for a business role.

You can delegate responsibility for the following role classes:

- Departments
- Cost centers
- Locations
- Selected business roles
- IT Shop structures (owner)

Example: During their vacation, user A delegates any responsibilities as manager of business roles with the "Projects 2222" role class and approval authorization for requests to their deputy, user B.

- A deputization, unlike single delegation, cannot be delegated further.
- A single responsibility that was acquired via deputization can be delegated further by single delegation. (Example: User B delegates their responsibility for the "Projects 2222: Role B" business role to User E.)
- An identity that is connected as a main or sub-identity cannot become a delegate nor can deactivated identities.

- **Single delegation**: Delegate your responsibility for a specific role or your memberships in a specific business or application role to any given identity.

  Example: User C delegates their membership in the "Project 2222: Role A" business role to user D.

  - Single delegations can be delegated further.

Delegations are automatically approved after a compliance check. They can be canceled and deleted. For more information about delegating tasks, see the *One Identity Manager Web Portal User Guide*.

Delegations are revoked when the valid-until date is exceeded, the delegate is deleted from the customer node, or the deputy is deactivated.

Detailed information about this topic

- Preparing single delegations on page 73
- Standard products for delegation on page 72
- Allowing delegation approvals on page 74
- Deleting request procedures and deputizations on page 205

Standard products for delegation

One Identity Manager provides standard products for delegations.

Table 20: Standard products for delegation

Service item	Shop | Shelf	Type of delegation
Deputy (temporary)	Identity & Access Lifecycle | Identity Lifecycle	Deputize
Delegation		Single delegations

In the default installation, all active One Identity Manager database identities are customers of the **Identity & Access Lifecycle** shop. This allows all enabled identities to delegate responsibilities.

Related topics

- Delegations on page 71
- Allowing delegation approvals on page 74

Preparing single delegations

Single delegations temporarily assign responsibilities for a specific role or memberships in a specific business or application role to any identity. This identity may further delegate responsibility or membership as needed.

To run single delegation in One Identity Manager

- In the Designer, set the **QER | ITShop | Delegation** configuration parameter.

  If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

The following objects in the default installation can be delegated.

- Responsibilities for:
  - Departments
  - Cost centers
  - Locations
  - Business roles
  - Identities
  - IT Shop Structures (owner)
- Membership in:

- Business roles
- Application roles

TIP: Specify the role classes associated to business roles for which memberships can be delegated. This option is available when the Business Roles Module is installed.

To permit single delegation of a role class

1. In the Manager, select the **Business roles > Basic configuration data > Role classes** category.
2. Select the role class in the result list.
3. Select the **Change main data** task.
4. Set **Delegable**.
5. Save the changes.

Use the Web Portal to delegate roles or responsibilities. For more information, see the *One Identity Manager Web Portal User Guide* and the *One Identity Manager Business Roles Administration Guide*.

Related topics

- Delegations on page 71

Allowing delegation approvals

Delegations are automatically approved after a compliance check. If delegations are going to be approved by an approver, assign a suitable approval policy to the default service item. This means that delegation also go through the defined approval process.

To approve deputization by an approver

1. In the Manager, select the **IT Shop > Service catalog > Predefined** category.
2. In the result list, select the **Deputy (temporary)** service item then select the **Change main data** task.
3. In the **Approval policy** field, select an approval policy.
4. Save the changes.

To approve single delegation by an approver

1. In the Manager, select the **IT Shop > Service catalog > Predefined** category.
2. In the result list, select the **Delegation** service item and select the **Change main data** task.
3. In the **Approval policy** field, select an approval policy.
4. Save the changes.

Related topics

- Delegations on page 71
- Standard products for delegation on page 72

Creating IT Shop requests from existing user accounts, assignments, and role memberships

You can create One Identity Manager requests for existing user accounts, membership in system entitlements, assignments to identities, and hierarchical roles when IT Shop goes into operation. One Identity Manager provides several methods to implement this. Using these methods, requests are created that are completed and approved. These requests can therefore be canceled at a later date. In addition to the initial request data, you can run a custom script from each method that sets other custom properties for a request.

Table 21: Methods for transforming direct assignments into requests

Method	Description
CreateITShopOrder (string CustomScriptName)	Creates a request from a direct assignment. This method can be applied to all tables used to find a `UID_Person`.
CreateITShopOrder (string uidOrgProduct, string uidPersonOrdered, string CustomScriptName)	Creates an assignment request from an assignment or membership. This method can be applied to all tables that cannot be used to find a `UID_Person`.
CreateITShopOrder (string uidOrgProduct, string uidWorkdeskOrdered, string uidPersonOrdered, string CustomScriptName)	Creates an assignment request from an assignment or membership and, in addition, saves a `UID_WorkdeskOrdered` with the request procedure.
CreateITShopWorkdeskOrder (string uidPerson, string CustomScriptName)	Creates a request for a workdesk from a direct assignment. This method can be applied to the `WorkDeskHasApp`, `WorkDeskHasESet` and `WorkDeskHasDriver` tables.

To run the methods

1. Create a script in the Designer with the Script Editor to call the desired method.

   You can find an example script for calling a Customizer method in VB syntax on the One Identity Manager installation medium in the

`Modules\QBM\AddOn\SDK\ScriptSamples\03 Using database objects\11 Call database object methods.vb` directory. You can use this example script as a template to create a script for call the methods described here.

2. Run the script.

   You can use the script test from the Script Editor to do this.

For more information about creating scripts, see the *One Identity Manager Configuration Guide*.

If a custom script is included in the method call, then this script will be run immediately before the request is saved in the database.

An example of a custom script

```
Public Sub CCC_AddCustomPropToRequest(ByRef dbSource As IEntity, ByRef
dbPWO As IEntity)
 'Populate values in PWO:
 dbPWO.PutValue("OrderReason", "Group membership assignment converted to
IT Shop request automatically.")
 End Sub
```

- `dbSource`: Refers to the source object. For example, `ADSAccountInADSGroup`, if memberships in Active Directory groups are to be converted in requests.
- `dbPWO`: Refers to the request to be generated.

Creating requests for identities

You can create requests for identities or memberships in system entitlements with `CreateITShopOrder (string CustomScriptName)`. Prepare the IT Shop accordingly in order to create the requests.

To create requests from direct assignments to identities or memberships in system entitlements

1. Prepare the company resources or system entitlements for use in the IT Shop.
2. Assign the company resources or system entitlements to a shelf in the IT Shop.
3. Link each user account for whose memberships requests are to be created with an identity.
4. Add identities as customers to shops to which the company resources or system entitlements are assigned as products.
5. (Optional): Create a script that populates other properties of the requests.
   - Pass the script name as a `CustomScriptName` parameter to the task.

6. Create a script to run `CreateITShopOrder (CustomScriptName string)` for the affected tables.

One Identity Manager creates requests from direct assignments for user accounts in the following way:

1. Determine identities and their assigned company resources.
2. Determine shops assigned to company resources and identities.
3. Create the requests with initial data.
4. Run custom scripts.
5. Save the requests (entry in the `PersonWantsOrg` table).
6. Assign identities to the product structure (entry in `PersonInITShopOrg` table).
7. Transform direct company resource assignments into indirect assignments to identities (for example, in the `PersonHasQERResource` table).

One Identity Manager creates requests for memberships in system entitlements in the following way:

1. Establish the user accounts and their memberships.
2. Determine the affected identities.
3. Determine the shops to which identities and the system entitlements are assigned.
4. Create the requests with initial data.
5. Run custom scripts.
6. Save the requests (entry in the `PersonWantsOrg` table).
7. Assign identities to the product structure (entry in `PersonInITShopOrg` table).
8. Transform direct company memberships into indirect memberships for affected user accounts (for example, in the `ADSAccountInADSGroup` table).

Related topics

- Preparing products for requesting on page 21

Creating user account requests

To assign user accounts to identities, use One Identity Manager account definitions. You can request matching account definitions for existing user accounts linked to the identities through the IT Shop. To create these requests, you can use `CreateITShopOrder (string CustomScriptName)`. This method can be used for all user account tables (for example, `ADSAccount` or `SAPUser`) and for the `ADSContact`, `EX0MailBox`, `EX0MailContact`, and `EX0MailUser`.

Prepare the IT Shop accordingly in order to create the requests.

To create requests for user accounts

1. Create an account definition for the target system. Assign the account definition to the target system.

   This account definition is used for all user accounts where no account definition is entered. You can miss out this step if all the user accounts are already assigned an account definition.
2. Prepare the account definition for use in the IT Shop.
3. Assign the account definition to a shelf in the IT Shop.
4. Link the user accounts to an identity, if there is no identity already linked.
5. Add identity as customers to shops to which the account definition is assigned as product.
6. (Optional): Create a script that populates other properties of the requests.
   - Pass the script name as a `CustomScriptName` parameter to the task.
7. Create a script that runs the method for the tables affected.

One Identity Manager creates requests for user accounts in the following way:

1. Determine the valid account definition.

   If an account definition is already assigned to the user account, it will be used. Otherwise, the account definition of the target system is used.
2. Determine the affected identities.
3. Determine the shops to which identities and the account definition are assigned.
4. Create the requests with initial data.
5. Run custom scripts.
6. Save the requests (entry in the `PersonWantsOrg` table).
7. Assign identities to the product structure (entry in `PersonInITShopOrg` table).
8. Transform any possible direct account definition assignments to indirect assignments (entry in `PersonHasTSBAccountDef` table).

Related topics

- Preparing products for requesting on page 21

Creating workdesk requests

Requests for workdesks are created with `CreateITShopWorkdeskOrder (string uidPerson, string CustomScriptName)`. Prepare the IT Shop accordingly in order to create the requests.

To create requests from assignments to workdesks

1. Prepare the company resources (software, system role, or driver) for use in the IT Shop.
2. Assign the company resources to a shelf in the IT Shop.
3. Select an identity as requester for the assignment to workdesks.
    - Pass this identity's `UID_Person` as a `uidPerson` parameter to the task.
4. Add the selected identity as a customer to the shops to which the company resources are assigned as products.
5. (Optional): Create a script that populates other properties of the requests.
    - Pass the script name as a `CustomScriptName` parameter to the task.
6. Create a script to run `CreateITShopWorkdeskOrder (string uidPerson, string CustomScriptName)` for the affected tables.

One Identity Manager creates requests for workdesk requests in the following way:

1. Determine workdesks and their assigned company resources.
2. Determine requester from the `uidPerson` parameter.
3. Determine shops assigned to company resources and requester.
4. Create the requests with initial data.
5. Run custom scripts.
6. Save the requests (entry in the `PersonWantsOrg` table).
7. Assign identities to the product structure (entry in `PersonInITShopOrg` table).
8. Transform direct company resource assignments into indirect assignments to workdesks (for example, in the `WorkDeskHasApp` table).

TIP: To create an identity that can be used as a requester when creating a workstation, set the **Hardware | Workdesk | WorkdeskAutoPerson** configuration parameter in the Designer. The following properties are used for the identity:

- Last name: **`Name of the workdesk`** (`Ident_Workdesk`)
- First name: **`Machine`**
- Identity type: **`Machine identity`** (`Machine`)

When the workstation is deleted, the associated identity is also deleted.

Related topics

- Preparing products for requesting on page 21

Creating assignment requests

You can create assignment requests for existing company resource assignments to hierarchical roles and for memberships of identities, devices, or workdesks in hierarchical roles. The following methods are available.

Table 22: Methods for transforming direct assignments into assignment requests

Method	Description
CreateITShopOrder (string uidOrgProduct, string uidPersonOrdered, string CustomScriptName)	Creates an assignment request from an assignment or membership. This method can be applied to all tables which cannot be used to find a `UID_Person`.
CreateITShopOrder (string uidOrgProduct, string uidWorkdeskOrdered, string uidPersonOrdered, string CustomScriptName)	Creates an assignment request from an assignment or membership and, in addition, saves a `UID_WorkdeskOrdered` with the request procedure.

Prepare the IT Shop accordingly in order to create the requests.

To create assignment requests from direct assignment to hierarchical roles and role memberships

1. From the **IT Shop > Identity & Access Lifecycle > Shelf: Identity Lifecycle** shelf, select an assignment resource.
    - Pass the product's `UID_ITShopOrg` as the `uidOrgProduct` parameter to the method.
2. From the customer node of the **IT Shop | Identity & Access Lifecycle** shop, select an identity as a requester for the assignment request.
    - Pass this identity's `UID_Person` as a `uidPersonOrdered` parameter to the method.
3. (Optional): Create a script that populates other properties of the requests.
    - Pass the script name as a `CustomScriptName` parameter to the method.
4. Create a script to run the `CreateITShopOrder (string uidOrgProduct, string uidPersonOrdered, string CustomScriptName)` method for the affected tables.

TIP: You can also create your own assignment resource and assign it to a shelf in any shop. Select an identity as requester for the assignment request from this shop's customer node. For more information, see Customizing assignment requests on page 64.

One Identity Manager creates assignment requests from existing assignments to hierarchical roles as follows:

1. Determine the hierarchical roles and their assigned company resources and identities (identities, devices, or workdesks).
2. Determine the requester from the `uidPersonOrdered` parameter.
3. Determine the assignment resource from the `uidOrgProduct` parameter.
4. Determine shops assigned to the assignment resource and requester.
5. Create the requests with initial data.
6. Run custom scripts.
7. Save the requests (entry in the `PersonWantsOrg` table).
8. Transform direct company resource assignments to hierarchical roles into indirect assignments to workdesks (for example, in the `DepartmentHasQERResource`) table. Transform direct company memberships to hierarchical roles into indirect memberships (for example, in the `PersonInDepartment`) table.

If the assignment request is to be created for a workdesk, pass the method the workdesk's `UID_WorkDesk` as `uidWorkdeskOrdered` parameter. The method saves this UID as `UID_WorkdeskOrdered` in the request (`PersonWantsOrg` table).

Detailed information about this topic

- Standard products for assignment requests on page 60

Related topics

- Preparing products for requesting on page 21

Adding system entitlements automatically to the IT Shop

The following steps can be used to automatically add system entitlements to the IT Shop. Synchronization ensures that the system entitlements are added to the IT Shop. If necessary, you can manually start synchronization with the Synchronization Editor. New system entitlements created in One Identity Manager also are added automatically to the IT Shop.

To add system entitlements automatically to the IT Shop

1. In the Designer, set the configuration parameter for automatically adding system entitlements to the IT Shop depending on existing modules.

   Example: **QER | ITShop | AutoPublish | ADSGroup** and **QER | ITShop | AutoPublish | ADSGroup | ExcludeList**

   List of relevant configuration parameters

- For disabled Microsoft Entra ID service plans:
  - QER | ITShop | AutoPublish | AADDeniedServicePlan
  - QER | ITShop | AutoPublish | AADDeniedServicePlan | ExcludeList
- For Microsoft Entra ID groups:
  - QER | ITShop | AutoPublish | AADGroup
  - QER | ITShop | AutoPublish | AADGroup | ExcludeList
- For Microsoft Entra ID subscriptions:
  - QER | ITShop | AutoPublish | AADSubSku
  - QER | ITShop | AutoPublish | AADSubSku | ExcludeList
- For Active Directory groups:
  - QER | ITShop | AutoPublish | ADSGroup
  - QER | ITShop | AutoPublish | ADSGroup | ExcludeList
  - QER | ITShop | AutoPublish | ADSGroup | AutoFillDisplayName

  If Active Roles Self-Service Manager is used:
  - TargetSystem | ADS | ARS_SSM
- For Exchange Online mail-enabled distribution groups:
  - QER | ITShop | AutoPublish | O3EDL
  - QER | ITShop | AutoPublish | O3EDL | ExcludeList
- For Microsoft 365 groups:
  - QER | ITShop | AutoPublish | O3EUnifiedGroup
  - QER | ITShop | AutoPublish | O3EUnifiedGroup | ExcludeList
- For Microsoft Teams teams:
  - QER | ITShop | AutoPublish | O3TTeam
  - QER | ITShop | AutoPublish | O3TTeam | ExcludeList
- For PAM user groups:
  - QER | ITShop | AutoPublish | PAGUsrGroup
  - QER | ITShop | AutoPublish | PAGUsrGroup | ExcludeList
- For SharePoint groups:
  - QER | ITShop | AutoPublish | SPSGroup
  - QER | ITShop | AutoPublish | SPSGroup | ExcludeList
- For OneLogin roles:
  - QER | ITShop | AutoPublish | OLGRole
  - QER | ITShop | AutoPublish | OLGRole | ExcludeList

2. Compile the database.

The system entitlements are added automatically to the IT Shop from now on.

The following steps are run to add a system entitlement to the IT Shop.

1. A service item is determined for the system entitlement.

   The service item is tested for each system entitlement and modified if necessary. The name of the service item corresponds to the name of the system entitlement.

   - The service item is modified if the system entitlement has a service item.
   - System entitlements without a service item are allocated a new service item.

2. The service item is assigned to one of the default service categories.
3. An application role for product owners is determined and the service item is assigned. For more information, see the administration manuals for the respective target system connection.

   Product owners can approve requests for membership in these system entitlements.

4. The system entitlement is labeled with the **IT Shop** option and assigned to the corresponding IT Shop shelf in the **Identity & Access Lifecycle** shop.

Subsequently, the shop's customers can request memberships in system entitlement through the Web Portal.

NOTE: When a system entitlement is irrevocably deleted from the One Identity Manager database, the associated service item is also deleted.

Related topics

- Entering service items on page 22
- Deleting unused application roles for product owners on page 83
- Product owners on page 216

Deleting unused application roles for product owners

The list of product owner application roles can quickly become confusing when groups are automatically added to the IT Shop. This is because an application role is added for each account manager. These application roles are no longer required when a groups are deleted.

Redundant application roles for product owners can be deleted through a scheduled process task. This deletes all the application role from the database for which the following applies:

- The parent application role is **Request & Fulfillment | IT Shop | Product owner**.
- The application role is not assigned to a service item.
- The application role is not assigned to a service category.
- The application role does not have members.

To display no longer required application roles with members

- In the Manager, select the **IT Shop > Troubleshooting > Orphaned product owners** category.

To delete application roles automatically

- In the Designer, configure and enable the **Cleans up application role "Request & Fulfillment | IT Shop | Product owners”** schedule.

NOTE: If you have set up your own application roles under the **Request & Fulfillment | IT Shop | Product Owner** application role that you use for custom use cases (tables), then check whether these can be deleted automatically. Otherwise, disable the **Clean up application role "Request & Fulfillment\IT Shop\Product owners"** schedule.

Related topics

- Adding system entitlements automatically to the IT Shop on page 81
- Product owners on page 216

2

Approval processes for IT Shop requests

All IT Shop requests are subject to a defined approval process. During this approval process, authorized identities grant or deny approval for the product assignments. You can configure this approval process in various ways and therefore customize it to meet your company policies.

You define approval policies and approval workflows for approval processes. Specify which approval workflows are going to be used for the request in the approval policies. Use approval workflows to specify which identity is authorized to grant or deny approval for the request at the time it was placed. An approval workflow can contain a number of approval levels, and this can, in turn, contain several approval steps, for example, when several management hierarchy layers need to give approval for a request. A special approval procedure is used to determine the approvers in each approval procedure.

In the default installation, different default approval policies are assigned to the **Identity & Access Lifecycle** shop. Therefore, requests from this shop are run through predefined approval processes. Assign an approval policy to the shop, the shelf or the service item of the **Identity & Access Lifecycle** shelf if requests from this shop should go through customized approval process.

Detailed information about this topic

- Approval policies for requests on page 85
- Approval workflows for requests on page 90
- Editing approval levels on page 94
- Default approval procedures on page 105

Approval policies for requests

One Identity Manager uses approval policies to determine the approver for each request process.

To edit an approval policy

1. In the Manager, select the **IT Shop > Basic configuration data > Approval policies** category.
2. Select an approval policy in the result list and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the approval policy main data.
4. Save the changes.

Related topics

- General main data of approval policies on page 86
- Validity checking on page 88
- Adding to the IT Shop on page 88
- Copying approval policies on page 89
- Editing approval workflows on page 88
- The approval policy overview on page 90

General main data of approval policies

Enter the following main data of an approval policy. If you add a new approval step, you must fill out the compulsory fields.

Table 23: General main data of approval policies

Main data	Meaning
Approval policies	Approval policy name.
Role type	Role type to determine inheritance of approval policies within an IT Shop solution. Add the required role types in **IT Shop > Basic configuration data > Roles types** category.
Priority	An integral number with a maximum of one digit. A priority is used to decided which approval policy should be used if several approval policies are found to be valid following the given rules. The highest priority has the largest number.
Approval workflow	Workflow for determining approvers when a product is requested. Select any approval workflow from the drop-down or click to set up a new workflow.

Main data	Meaning
Renewal workflow	Approval workflow for determining approvers when a product is renewed. Select any approval workflow from the drop-down or click to set up a new workflow. If no renewal workflow is specified, the approval workflow of the request is used when the request is renewed (`UID_SubMethodOrderProduct`).
Cancellation workflow	Approval workflow for determining approvers when a requested product is canceled. Select any approval workflow from the drop-down or click to set up a new workflow. If there is no cancellation workflow given, cancellation is approved immediately.
Mail templates	Mail template used for creating email notifications for granting or denying approval for a request and extended, expired, or canceled requests.
Description	Text field for additional explanation.
Do not show	Specifies whether this approval policy is hidden in the Web Portal.

Detailed information about this topic

- Determining effective approval policies on page 103
- Role types for the IT Shop on page 212
- Setting up approval workflows on page 93
- Notifications in the request process on page 181

Default approval policies

One Identity Manager supplies service items by default. These approval policies are used in the **Identity & Access Lifecycle** shop approval processes. You can store mail templates with default approval policies for sending notifications during the request process and specifying a priority.

To edit default approval policies

- In the Manager, select the **IT Shop > Basic configuration data > Approval policies > Predefined** category.

Adding to the IT Shop

You can assign approval policies to shops, shopping centers, or shelves. The approval policy is applied to the request from the respective IT Shop nodes if there are no approval policies assigned to child IT Shop nodes. For more information, see Determining effective approval policies on page 103.

To assign an approval policy to shops, shopping centers, or shelves

1. In the Manager, select the **IT Shop > Basic configuration data > Approval policies** category.
2. In the result list, select the approval policy.
3. Select the **Add to IT Shop** task.

   In the **Add assignments** pane, assign the shops, shopping centers, or shelves.

   > TIP: In the **Remove assignments** pane, you can remove shop, shopping center, or shelf assignments.
   >
   > ***To remove an assignment***
   >
   > Select the shop, shopping center, or shelf and double-click ✓.
4. Save the changes.

Validity checking

Once you have edited an approval policy, you need to test it. This checks whether the approval steps can be used in the approval workflows in this combination. Non-valid approval steps are displayed in the error window.

To test an approval policy

1. In the Manager, select the **IT Shop > Basic configuration data > Approval policies** category.
2. Select the approval policy in the result list.
3. Select the **Validity check** task.

Editing approval workflows

You can edit approval workflow that are assigned an approval policy here.

To edit approval workflow properties

1. In the Manager, select the **IT Shop > Basic configuration data > Approval policies** category.
2. Select the approval policy in the result list.
3. To edit the approval workflow for requests, select task **1. Edit approval workflow**.
4. To edit the renewal workflow for requests, select task **2. Edit approval workflow**.
5. To edit the cancellation workflow, select task **3. Edit approval workflow**.
6. This opens the Workflow Editor.

Detailed information about this topic

- Working with the Workflow Editor on page 90

Copying approval policies

To customize pre-defined approval polices, you can copy approval policies and then edit them. All assigned approval workflows are copied as well.

To copy an approval policy

1. In the Manager, select the **IT Shop > Basic configuration data > Approval policies** category.
2. Select an approval policy in the result list and run the **Change main data** task.
3. Select the **Copy approval policies** task.
4. Enter a name for the copy of the approval policy.
5. Enter names for the workflow copies.

   The **Self service** workflow is not copied, but assigned to the copy of the approval policy as in the original.
6. Click **OK** to start copying.

   - OR -

   Click **Cancel** to cancel copying.
7. To edit the copy immediately, click **Yes**.

   - OR -

   To edit the copy later, click **No**.

Related topics

- Approval policies for requests on page 85

The approval policy overview

On the overview form, you see, at a glance, the most important information about an approval policy.

To obtain an overview of an approval policy

1. In the Manager, select the **IT Shop > Basic configuration data > Approval policies** category.
2. Select the approval policy in the result list.
3. Select the **Approval policy overview** task.

Approval workflows for requests

You need to allocate an approval workflow to the approval policies in order to find the approvers. In an approval workflow, you specify the approval procedures, the number of approvers and a condition for selecting the approvers.

Use the Workflow Editor to create and edit approval workflows.

To edit an approval workflow

1. In the Manager, select the **IT Shop > Basic configuration data > Approval workflows** category.
2. Select the approval workflow in the result list and run the **Change main data** task.

   - OR -

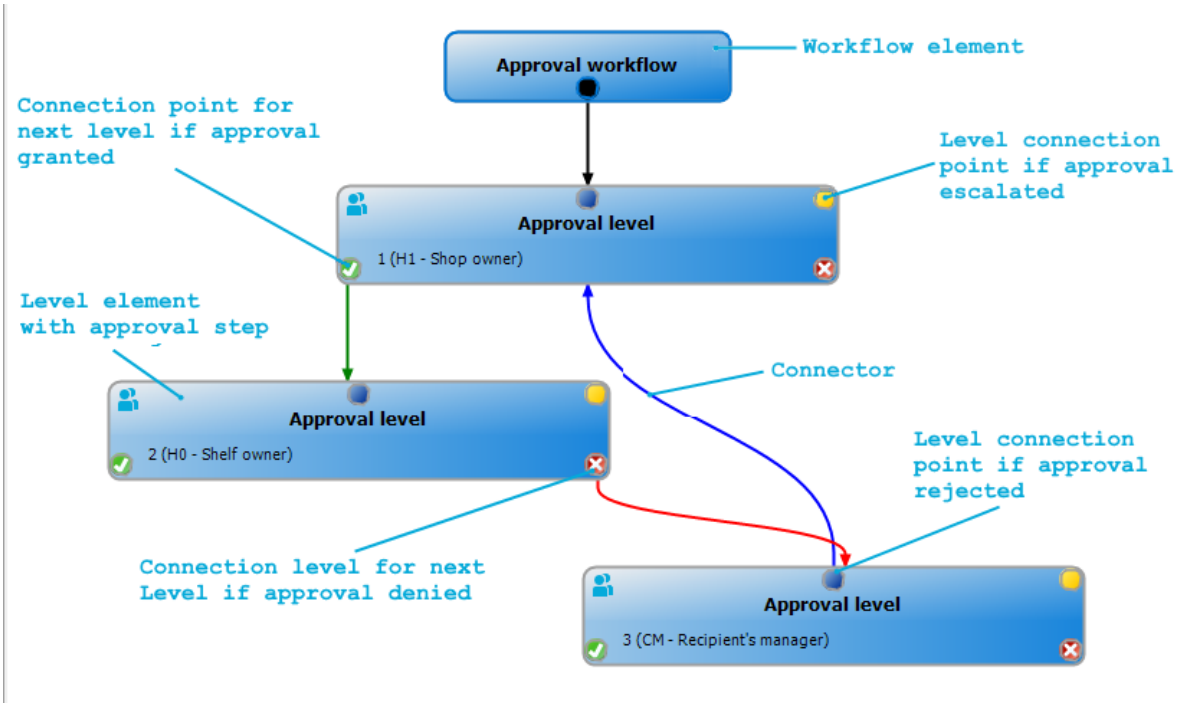
   Click in the result list.

   This opens the Workflow Editor.
3. Edit the approval workflow main data.
4. Save the changes.

Working with the Workflow Editor

Use the Workflow Editor to create and edit approval workflows. The Workflow Editor allows approval levels to be linked together. Multi-step approval processes are clearly displayed in a graphical form.

Figure 4: Workflow Editor



Approval levels and approval steps belonging to the approval workflow are edited in the Workflow Editor using special control elements. The Workflow Editor contains a toolbox. The toolbox items are activated or deactivated depending on how they apply to the control. You can move the layout position of the control elements in the Workflow Editor with the mouse or these can be moved automatically.

Table 24: Entries in the toolbox

Control	Item	Meaning
Workflow	Edit	Edit the properties of the approval workflow.
	Layout automatically	The workflow elements are aligned automatically. The workflow layout is recalculated.
Approval levels	Add	A new approval level is added to the workflow.
	Edit	Edit the properties of the approval workflow.
	Delete	Deletes the approval level.
Approval steps	Add	Add a new approval step to the approval level.
	Edit	Edit the properties of the approval step.
	Delete	Deletes the approval step.
Assignments	Remove positive	The **Approved** connector for the selected approval level is deleted.

Control	Item	Meaning
	Remove negative	The **Deny** connector for the selected approval level is deleted.
	Remove reroute	The **Reroute** connector for the selected approval level is deleted.
	Remove escalation	The **Escalate** connector for the selected approval level is deleted.

Each of the controls has a properties window for editing the data of the approval workflow, level, or step. To open the properties window, select the **Toolbox > <Control> > Edit** item.

To delete a control, select the element and then the **Toolbox > <Control> > Delete** item.

Individual elements are linked to each other with a connector. Activate the connection points with the mouse. The cursor changes into an arrow icon for this. Hold down the left mouse button and pull a connector from one connection point to the next.

Figure 5: Approval workflow connectors

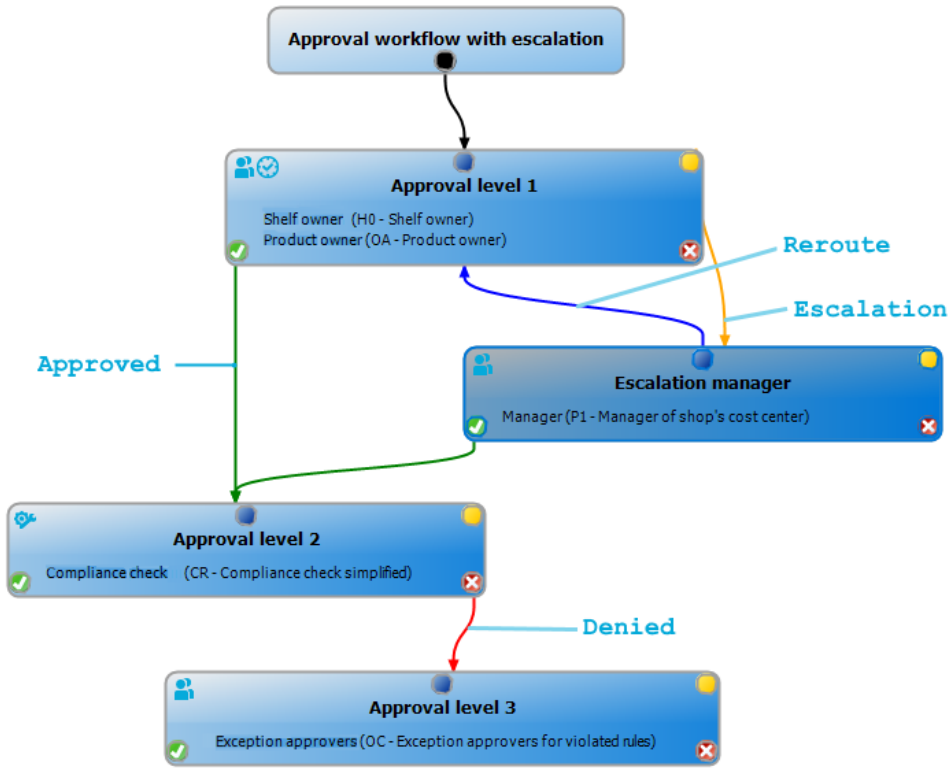


Table 25: Approval workflow connectors

Connector	Meaning
Approve	Link to next approval level if the current approval level was granted approval.
Deny	Link to next approval level if the current approval level was not granted approval.
Reroute	Link to other approval levels to bypass the current approval.
Escalation	Connection to another approval level when the current approval level is escalated after timing out.

By default, a connection between workflow elements and level elements is created immediately when a new element is added. If you want to change the level hierarchy, drag a new connector to another level element.

Alternatively, you can release connectors between level elements using the **Toolbox > Assignments** items. To do this, mark the level element where the connector starts. Then add a new connector.

Different icons are displayed on the level elements depending on the configuration of the approval steps.

Table 26: Icons on the level elements

Icon	Meaning
	The approval decision is made by the system.
	The approval decision is made manually.
	The approval step contains a reminder function.
	The approval step contains a timeout.

Changes to individual elements in the workflow do not take place until the entire approval workflow is saved. The layout position in the Workflow Editor is saved in addition to the approval policies.

Setting up approval workflows

An approval workflow consists of one or more approval levels. An approval level can contain one approval step or several parallel approval steps. Within the approval process, all of the approval steps for one approval level must be run before the next approval level is called. Use connectors to set up the sequence of approval levels in the approval workflow.

When you add a new approval workflow, the first thing to be created is a new workflow element.

To edit approval level properties

1. Open the Workflow Editor.
2. Select the **Toolbox > Workflow > Edit** item.
3. Edit the workflow properties.
4. Click **OK**.

Table 27: Approval workflow properties

Property	Meaning
Name	Approval workflow name.
System halt (days)	Number of days to elapse after which the approval workflow, and therefore the system, automatically halts the entire approval process.
Description	Text field for additional explanation.

Detailed information about this topic

- Halting a request on timeout on page 160

Editing approval levels

An approval level provides a method of grouping individual approval steps. All the approval steps in one approval level are run in parallel. All the approval steps for different approval levels are run one after the other. You use the connectors to specify the order.

Specify the individual approval steps in the approval levels. At least one approval step is required per level. Enter the approval steps first before you add an approval level.

To add an approval level

1. Select the **Toolbox > Approval levels > Add** item.

   This opens the properties dialog for the first approval step.
2. Enter the approval step properties.
3. Save the changes.

You can edit the properties of an approval level as soon as you have added an approval level with at least one approval step.

To edit approval level properties

1. Select the approval level.
2. Select the **Toolbox > Approval levels > Edit** item.
3. Enter a display name for the approval level.
4. Save the changes.

NOTE: You can define more than one approval step for each approval level. In this case, the approvers of an approval level can make a decision about a request in parallel rather than sequentially. The request cannot be presented to the approvers at the next approval level until all approval steps of an approval level have been completed within the approval process.

To add more approval steps to an approval level

1. Select the approval level.
2. Select the **Toolbox > Approval steps > Add** item.
3. Enter the approval step properties.
4. Save the changes.

Detailed information about this topic

- Properties of an approval step on page 95
- Editing approval steps on page 95

Editing approval steps

To edit approval level properties

1. Select the approval step.
2. Select the **Toolbox > Approval steps > Edit** item.
3. Edit the approval step properties.
4. Save the changes.

Detailed information about this topic

- Properties of an approval step on page 95

Properties of an approval step

On the **General** tab, enter the data described below. On the **Mail templates** tab, select the mail templates for generating mail notifications. If you add a new approval step, you must fill out the required fields.

Table 28: General properties of an approval step

Property	Meaning
Single step	Approval step name.
Approval	Procedure to use for determining the approvers.

Property	Meaning
procedure	
Processing status	Processing status of the success or failure case of the approval step. The processing status for the request is set according to the decision and whether it has been made positively or negatively. Define the processing status in the basic configuration data.
Role	Hierarchical role from which to determine the approvers. The role is used in the OM and OR default approval procedures. Additionally, you can use the role if you use a custom approval procedure in the approval step.
Fallback approver	Application role whose members are authorized to approve requests if an approver cannot be determined through the approval procedure. Assign an application from the drop-down. To create a new application role, click . Enter the application role name and assign a parent application role. For more information, see the *One Identity Manager Authorization and Authentication Guide*. NOTE: The number of approvers is not applied to the fallback approvers. The approval step is considered approved the moment as soon as one fallback approver has approved the request.
Condition	Condition for calculating the approval decision. The condition is used in the CD, EX, or WC default approval procedures. Additionally, you can use the role if you use a custom approval procedure in the approval step. Comparison value for the risk index in the approval procedure RI. Enter a number in the range 0.1 to 1.0. 1.0. You can use **,** or **.** as a decimal point.
Number of approvers	Number of approval required to approve a request. Use this number to further restrict the maximum number of approvers of the implemented approval procedure. If there are several identities allocated as approvers, then this number specifies how many identities from this group have to approve a request. A request can only be passed on to the next level if this has been done. If you want approval decisions to be made by all the identities found using the applicable approval procedure, for example, all members of a role (default approval procedure OR), enter the value **-1**. This overrides the maximum number of approvers defined in the approval procedure. If not enough approvers can be found, the approval step is presented to the fallback approvers. The approval step is considered approved as soon as one fallback approver has approved the request. If an approval decision is made by the chief approval team, it overrides the approval decision of just one regular approver. This means, if three approvers must approve an approval step and the chief approval team

Property	Meaning
	makes a decision, two more are still required. The number of approvers defined in an approval step is not taken into account in the approval procedures CD, EX,or WC.
Description	Text field for additional explanation.
Approval reason	Reason entered in the request if approval is automatically granted. This field is only shown for the approval procedures CD, CR, RI, SB, EX, and WC. In the CR approval procedure, you can user the wild card **{0}** in the text. The place holder syntax corresponds to a format place holder in VB.Net ({0} to {9})
Reject reason	Reason entered in the request and the approval history, if approval is automatically denied. This field is only shown for the approval procedures CD, CR, RI, SB, EX, and WC. In the CR approval procedure, you can user the wild card **{0}** in the text. The place holder syntax corresponds to a format place holder in VB.Net ({0} to {9})
Reminder after	Time interval after which the approver is notified by mail that there are still pending requests for approval. The input is converted into working hours and displayed additionally. • From the drop-down, select the unit of time and enter an appropriate value. NOTE: Ensure that a state, county, or both is entered into the identity's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating identities' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*. TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*. If more than one approver was found, each approver will be notified. The same applies if an additional approver has been assigned. If an approver delegated the approval, the time point for reminding the delegation recipient is recalculated. The delegation recipient and all the other approvers are notified. The original approver is not notified. If an approver has made an inquiry, the time point for reminding the queried identity is recalculated. As long as the inquiry has not been

Property	Meaning
	answered, only this identity is notified.
Timeout	Time interval after which the approval step automatically handles the approval decision. The input is converted into working hours and displayed additionally. • From the drop-down, select the unit of time and enter an appropriate value. The working hours of the respective approver are taken into account when the time is calculated. NOTE: Ensure that a state, county, or both is entered into the identity's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating identities' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*. TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*. If more than one approver was found, then an approval decision for the approval step is not automatically made until the timeout for all approvers has been exceeded. The same applies if an additional approver has been assigned. If an approver delegated approval, the time point for automatic approval is recalculated for the new approver. If this approval is rejected, the time point for automatic approval is recalculated for the original approver. If an approver is queried, the approval decision must be made within the defined timeout anyway. The time point for automatic approval is not recalculated. If additional approvers are determined by recalculating the current approvers, then the automatic approval deadline is not extended. The additional approvers must approve within the time frame that applies to the current approver.
Timeout behavior	Action that is run if the timeout expires. • **Approved**: The request is approved in this approval step. The next approval level is called. • **Deny**: The request is denied in this approval step. The approval level for denying is called.

Property	Meaning
	• **`Escalation`**: The request process is escalated. The escalation approval level is called. • **`Cancel`**: The approval step, and therefore the entire approval process for the request, is canceled.
Reason type on approval	Specifies which type of reason is required when granting approval to this approval step. • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Reason type on denial	Specifies which type of reason is required when denying approval to this approval step. • Optional: A reason can be provided if required. • Reason required (standard or free): A standard reason must be selected or a reason given with any text. • Free text required: A reason must be given with freely selected text.
Additional approver possible	Specifies whether a current approver is allowed to instruct another identity as an approver. This additional approver has parallel authorization to make approvals for the current request. The request is not passed on to the next approval level until both approvers have made a decision. This option can only be set for approval levels with a single, manual approval step.
Approval can be delegated	Specifies whether a current approver can delegate the approval of the request to another identity. This identity is added to the current approval step as the approver and then makes the approval decision instead of the approver who delegated. This option can only be set for approval levels with a single, manual approval step.
Approval by affected identity	Specifies whether the identity that is affected by the approval decision can also approve this attestation case. If this option is set, requester, and request recipients can approve the request. If this option is not set, use the **QER | ITShop | PersonInsertedNoDecide**, **QER | ITShop | PersonOrderedNoDecide**, **QER | ITShop | PersonInsertedNoDecideCompliance**, and **QER | ITShop | PersonOrderedNoDecideCompliance** configuration parameters to specify for all requests whether requester and request recipient can approve the request.

Property	Meaning
Do not show in approval history	Specifies whether or not the approval step should be displayed in the approval history. For example, this behavior can be applied to approval steps with the **CD - calculated approval** procedure, which are used only for branching in the approval workflow. It makes it easier to follow the approval history.
No automatic approval	Specifies whether the approval step is decided manually. The request is presented again to an approver even if they are the requester themselves or the request has been approved in a previous approval step. The setting of the **DecisionOnInsert**, **ReuseDecision** and **AutoDecision** configuration parameters is ignored in this approval step.
Escalate if no approver found	Specifies whether the approval step is escalated if no approver can be found and no fallback approver is assigned. In this case, the request is neither canceled nor passed to the chief approval team. This option can only be enabled if an approval level is linked to escalation. The option cannot be enables if the approval step uses the approval procedure OC or OH.

Detailed information about this topic

- Request risk analysis on page 132
- Notifications in the request process on page 181
- Processing status on page 208
- Reminding approvers on page 182
- Escalating an approval step on page 155
- Automatic approval on timeout on page 159
- Halting a request on timeout on page 160
- Automatically approving requests on page 144
- Entscheider über eine festgelegte Rolle ermitteln
- Waiting for further approval on page 120
- Approvals to be made externally on page 123
- Calculated approval on page 122

Related topics

- Selecting responsible approvers on page 105
- Approvers cannot be established on page 157
- Approval by the chief approval team on page 161
- Approving requests from an approver on page 142
- Restricting exception approvers on page 139

Connecting approval levels

When you set up an approval workflow with several approval levels, you have to connect each level with another. You may create the following links.

Table 29: Links to approval levels

Link	Description
Approve	Link to next approval level if the current approval level was granted approval.
Deny	Link to next approval level if the current approval level was not granted approval.
Reroute	Link to another approval level to bypass the current approval. Approvers can pass the approval decision through another approval level, for example, if approval is required by a manager in an individual case. To do this, create a connection to the approval levels to which the approval can be rerouted. This way, approvals can also be rerouted to a previous approval level, for example, if an approval decision is considered not to be well-founded. Starting from one approval level, more than one reroute can lead to different approval levels. The approvers select, in the Web Portal, which of these approval levels to reroute the approval to. It is not possible to reroute approval steps with the approval procedures OC, OH, EX, CR, CD, SB, or WC.
Escalation	Link to another approval level when the current approval level is escalated after timing out.

If there are no further approval levels after the current approval level, the request is considered approved if the approval decision was to grant approval. If approval is not granted, the request is considered to be finally denied. The approval process is closed in both cases.

Copying approval workflows

You can copy default approval workflows in order to customize them.

To copy an approval workflow

1. In the Manager, select the **IT Shop > Basic configuration data > Approval workflows** category.
2. Select an approval workflow in the result list and run the **Change main data** task.
3. Select the **Copy workflow** task.
4. Enter a name for the copy.

5. Click **OK** to start copying.

   - OR -

   Click **Cancel** to cancel copying.
6. To edit the copy immediately, click **Yes**.

   - OR -

   To edit the copy later, click **No**.

Deleting approval workflows

The approval workflow can only be deleted if it is not assigned to an approval policy.

To delete an approval workflow

1. Remove all assignments to approval policies.
   a. Check to which approval policies the approval workflow is assigned.
   b. Go to the main data form for the approval policy and assign a different approval workflow.
2. In the Manager, select the **IT Shop > Basic configuration data > Approval workflows** category.
3. Select an approval workflow in the result list.
4. Click .
5. Confirm the security prompt with **Yes**.

Detailed information about this topic

- The approval workflow overview on page 102
- General main data of approval policies on page 86

The approval workflow overview

To obtain an overview of an approval workflow

1. In the Manager, select the **IT Shop > Basic configuration data > Approval workflows** category.
2. Select the approval workflow in the result list.
3. Select **Approval workflow overview**.

Default approval workflows

One Identity Manager provides approval workflows by default. These approval workflows are used in the **Identity & Access Lifecycle** shop approval processes. Each default approval workflow is linked to a default approval policy. You can edit different properties of the approval step, for example, to configure notifications in the request process.

To edit default approval workflows

- In the Manager, select the **IT Shop > Basic configuration data > Approval workflows > Predefined** category.

Determining effective approval policies

You can apply approval policies to different IT Shop structures and service items. If you have multiple approval policies within your IT Shop, which policy is to be used is based on which rules are specified.

Effective approval policies are defined by the following steps: If no approval policy is found in a step, the next one is checked. The following objects are checked in the following sequence:

1. The requested service item
2. The service category to which this service item is assigned
3. Parent service category
4. The shelf used for requesting the service item
5. The shop where the shelf is located
6. The shopping center where the shop is located

Multiple approval policies can also be identified in this way.

An approval policy found by one of these methods is applied under the following conditions:

- The approval policy is not assigned a role type.

  - OR -

- The assigned role type corresponds to the shelf role type.

If more than one effective approval policies are identified by the rules, the effective approval policy is determined by the following criteria (in the given order).

1. The approval policy has the highest priority (alphanumeric sequence).
2. The approval policy has the lowest number of approval steps.
3. The first approval policy found is taken.

Furthermore:

- If no approval policy can be found for a product, a request cannot be started.

  The same applies for renewals and unsubscriptions.
- If no approver can be determined for one level of an approval policy, the request can be neither approved nor denied.
  - Pending requests are rejected and closed.
  - Unsubscriptions cannot be approved. Therefore, unsubscribed products remain assigned.
  - Renewals cannot be approved. Therefore, products for renewal remain assigned until the **valid until** date is reached.

NOTE: If an approval workflow for pending requests changes, you must decide how to proceed with these requests. Configuration parameters are used to define the desired procedure.

For more information, see Changing approval workflows of pending requests on page 176.

Related topics

- Approvers for renewals on page 104
- Approvers for unsubscriptions on page 105
- Requests with limited validity period on page 172

Approvers for renewals

Once the currently effective approval policy has been identified, the actual approvers are determined by the approval workflow specified by it. When requests are renewed, a renewal workflow is run. If no renewal workflow is stored with the approval policy, approvers are determined by the approval workflow.

If no approvers can be identified for a renewal, then the renewal is denied. The product remains assigned only until the **Valid until** date. The request is then canceled and the assignment is removed.

Related topics

- Canceling or unsubscribing requests on page 174
- Renewing requests on page 173
- Determining effective approval policies on page 103

Approvers for unsubscriptions

Once the currently effective approval policy has been identified, the actual approvers are determined by the approval workflow specified by it. When a product is unsubscribed, the cancellation workflow runs. If no unsubscribe workflow is stored with the approval policy, approvers are determined by the approval workflow.

If no approvers can be determined for an unsubscription, then the unsubscription is denied. The product remains assigned.

Related topics

- Determining effective approval policies on page 103

Selecting responsible approvers

One Identity Manager can make approvals automatically in an approval process or through approvers. An approver is an identity or a group of identities who can grant or deny approval for a request (renewal or cancellation) within an approval process. It takes several approval procedures to grant or deny approval. You specify in the approval step which approval procedure should be used.

If several people are determined to be approvers by an approval procedure, the number given in the approval step specifies how many people must approve the step. Only then is the request presented to the approvers in the next approval level. The request is canceled if an approver cannot be found for an approval step.

One Identity Manager provides approval procedures by default. You can also define your own approval procedures.

The DBQueue Processor calculates which identity is authorized as an approver and in which approval level. The calculation is triggered by the **IT Shop approver** schedule. Take into account the special cases for each approval procedure when setting up the approval workflows to determine those authorized to grant approval.

Default approval procedures

Default approval procedures are provided to help with selecting which approvers are responsible. These you can use to setup your own approval workflows.

To display default approval procedures

- In the Manager, select the **IT Shop > Basic configuration data > Approval procedures > Predefined** category.

For more information about default approval procedures for requests, see:

- BA - Owner of the application: Determining owners as approvers on page 110
- BE - Approver of the application entitlement: Determining special approvers on page 113
- BR - Back to recipient: Determining requester or recipients on page 118
- BS - Back to requester: Determining requester or recipients on page 118
- C3 - Identity in additional request data: Determining special identities as approvers on page 118
- CD - Calculated approval: Calculated approval on page 122
- CM - Recipient's manager:Determining request recipients as approvers on page 108
- CR - Compliance check (simplified): Compliance checking requests on page 134
- D0 - Manager of shelf's department: Determining managers or members of a role as approvers on page 108
- D1 - Manager of shop's department: Determining managers or members of a role as approvers on page 108
- D2 - Manager of shopping center's department: Determining managers or members of a role as approvers on page 108
- DI - Role approvers (IT) of the department given in the request: Determining special approvers on page 113
- DM - Manager of recipient's department: Determining request recipients as approvers on page 108
- DP - Manager of department provided in request: Determining managers or members of a role as approvers on page 108
- DR - Role approvers of the department given in the request: Determining special approvers on page 113
- EX - Approvals to make externally: Approvals to be made externally on page 123
- H0 - Shelf owner: Determining owners as approvers on page 110
- H1 - Shop owner: Determining owners as approvers on page 110
- H2 - Shopping center owner: Determining owners as approvers on page 110
- ID - Role approvers (IT) of recipient's department: Determining special approvers on page 113
- IL - Role approvers (IT) of recipient's location: Determining special approvers on page 113
- IO - Role approvers (IT) of recipient's primary business role: Determining special approvers on page 113
- IP - Role approvers (IT) of recipient's cost center: Determining special approvers on page 113
- KA - Product owner and additional owner of the Active Directory group: Determining owners as approvers on page 110

- MS - Manager of the role to request: Determining managers or members of a role as approvers on page 108
- OA - Product owner: Determining owners as approvers on page 110
- OC - Exception approvers for violated rules: Determining exception approvers on page 136
- OH - Exception approver for worst rule violation: Determining exception approvers on page 136
- OM - Manager of a specific role: Determining managers or members of a role as approvers on page 108
- OR - Members of a certain role: Determining managers or members of a role as approvers on page 108
- OT - Attestor of the service item to assign: Determining special approvers on page 113
- OX - Owner of the object in any request parameter of the request properties: Determining owners as approvers on page 110
- P0 - Manager of shelf's cost center: Determining managers or members of a role as approvers on page 108
- P1 - Manager of shop's cost center: Determining managers or members of a role as approvers on page 108
- P2 - Manager of shopping center's cost center: Determining managers or members of a role as approvers on page 108
- PA - Additional owner of the Active Directory group: Determining owners as approvers on page 110
- PG - Owner of requested privileged access: Determining owners as approvers on page 110
- PI - Role approvers (IT) of the cost center given in the request: Determining special approvers on page 113
- PM - Manager of recipient's cost center: Determining request recipients as approvers on page 108
- PP - Manager of cost center provided in request: Determining managers or members of a role as approvers on page 108
- PR - Role approvers of the cost center given in the request: Determining special approvers on page 113
- RD - Role approvers of the recipient's primary department: Determining special approvers on page 113
- RI - Identity's risk index: Request risk analysis on page 132
- RL - Role approvers of the recipient's primary location: Determining special approvers on page 113
- RO - Rule approver of the recipient's primary business role: Determining special approvers on page 113

- RP - Role approvers of the recipient's primary cost center: Determining special approvers on page 113
- SB - Self service: Automatic approvals on page 119
- TO - Target system manager of the system entitlement to request: Determining target system managers as approvers on page 117
- WC - Waiting for further approval: Waiting for further approval on page 120

Related topics

- Setting up approval procedures on page 125
- Determining the responsible approvers on page 130

Determining request recipients as approvers

Use the following approval procedure if you want to determine the manager of the request recipient to be the approver.

CM - Recipient's manager

The request recipient is assigned a manager (`Person` table, `UID_PersonHead` column). This identity is determined as the approver.

DM - Manager of recipient's department

The request recipient is assigned a primary department (`Person` table, `UID_Department` column). A manager (`Department.UID_PersonHead`), deputy manager (`Department.UID_PersonHeadSecond`), or an application role for additional managers (`Department.UID_AERoleManager`) is assigned to this department. All the identities assigned here are determined as approvers.

PM - Manager of recipient's cost center

A primary cost center is assigned to the request recipient (`Person` table, `UID_Profitcenter` column). A manager (`Profitcenter.UID_PersonHead`), deputy manager (`Profitcenter.UID_PersonHeadSecond`), or an application role for additional managers (`Profitcenter.UID_AERoleManager`) is assigned to this cost center. All the identities assigned here are determined as approvers.

Related topics

- Default approval procedures on page 105

Determining managers or members of a role as approvers

Managers can be assigned to identities and hierarchical roles If these managers can approve requests, you can use the following approval procedures. In addition, members

with a specified hierarchical role can be determined as approvers.

D0 - Manager of shelf's department

A department is assigned to the shelf from which the request is made. The department is assigned a manager, a deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

D1 - Manager of shop's department

A department is assigned to the shop from which the request is made. The department is assigned a manager, a deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

D1 - Manager of shopping center's department

A department is assigned to the shopping center from which the request is made. The department is assigned a manager, a deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

DP - Manager of department given in the request

A department is entered in the request. This department is assigned a manager, a deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

P0 - Manager of shelf's cost center

A cost center is assigned to the shelf from which the request is made. This cost center is assigned a manager, deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

P1 - Manager of shop's cost center

A cost center is assigned to the shop from which the request is made. This cost center is assigned a manager, deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

P2 - Manager of shopping center's cost center

A cost center is assigned to the shopping center from which the request is made. This cost center is assigned a manager, deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

PP - Manager of cost center given in the request

A cost center is entered in the request. This cost center is assigned a manager, deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

MS - Manager of the role to request

Requests membership in or assignment to a hierarchical role (department, cost center, location, business role, application role). The role is assigned a manager, a deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

This approval procedure can only be used for assignment requests.

OM - Manager of a specific role

Determines approvers via a role (department, cost center, location, business role, application role) specified in the approval step. The role is assigned a manager, a deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

OR - Members of a certain role

Determines approvers via a role (department, cost center, location, business role, application role) specified in the approval step. All secondary members of this role are determined as approvers.

Related topics

- Default approval procedures on page 105
- Properties of an approval step on page 95

Determining owners as approvers

Special owners are assigned to various objects in One Identity Manager. Different approval procedures can be used to determine these owners as approvers.

H0 - Shelf owner

The shelf used for the request is assigned an owner, deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

H1 - Shop owner

The shop used for the request is assigned an owner, deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

H2 - Shopping center owner

The shopping center used for the request is assigned an owner, deputy manager, or an application role for additional managers. All the identities assigned here are determined as approvers.

OA - Product owner

The service item of the requested product is assigned an application role for product owners (`AccProduct` table, `UID_OrgRuler` column). All secondary members of this application are determined as approvers.

Use this approval procedure for assignment requests as well.

KA - Product owner and additional owner of the Active Directory Group

Installed modules: Active Roles Module

Effective when requesting: Active Directory Groups

The service item of the requested group is assigned an application role for product owners (`AccProduct` table, `UID_OrgRuler` column). All secondary members of this application are determined as approvers.

If the groups were added automatically to the IT Shop, the account managers are identified as product owners. For more information about these functions, see the *One Identity Manager Administration Guide for One Identity Active Roles Integration*. If the **TargetSystem | ADS | ARS_SSM** configuration parameters is set, the additional owners of the Active Directory group are determined (`ADSGroup` table, `edsvaSecondaryOwners` column).

PA - Additional owner of the Active Directory group

Installed modules: Active Roles Module

Effective when requesting: Active Directory Groups

Prerequisite: The **TargetSystem | ADS | ARS_SSM** configuration parameter is set. The **Additional owners** column (`ADSGroup.edsvaSecondaryOwners`) is only available in this particular case.

The additional owners of the requested group are determined as approvers. Identities are determined that are:

- Linked to the assigned Active Directory user account - or -
- A member in the assigned Active Directory group through their Active Directory user account

PG - owners of the requested privileged access request

Installed modules: Privileged Account Governance Module

Effective when requesting: Access requests for privileged objects of a Privileged Account Management system, such as PAM assets, PAM asset accounts, and PAM directory accounts.

An application role for owners (`UID_AERoleOwner` column) is assigned to the privileged object. All secondary members of this application are determined as approvers. The owners of the privileged objects must have the **Privileged Account Governance | Asset and account owners** application role or a child application role.

To make an access request, additional system prerequisites must be met by the Privileged Account Management system. For more information about PAM access requests, see the *One Identity Manager Administration Guide for Privileged Account Governance*.

BA - Owner of the application

Installed modules: Application Governance Module

Effective when requesting: Application entitlements

The application under which the requested application entitlement is published, is assigned an application role for owners (`AOBApplication` table, `UID_AERoleOwner` column). All secondary members of this application are determined as approvers. The application owners must be assigned to the **Application Governance | Owners** application role or a child application role.

For more information about applications and application entitlements, see the *One Identity Manager Application Governance User Guide*.

OX - Owner of the object in any request parameter of the request properties

Effective for: Requests with request parameters

Prerequisites:

- There is a multi requestable/unsubscribable resource for use in the IT Shop.
- There is a service item for this resource. This is a request property with at least one request parameter assigned (`AccProduct` table, `UID_AccProductParamCategory` table).
- The name of the request parameter is given in the approval step as well as the table column that references the application role.

The object to be requested is specified as an request parameter when the request is made. An application role for owners (`UID_AERoleOwner` column) is assigned to this object. All secondary members of this application are determined as approvers.

For more information, see Determining approvers via products requested by request parameter on page 112.

Related topics

- Default approval procedures on page 105

Determining approvers via products requested by request parameter

If the object to request is given as a request parameter in the request and the owners of the object are going to be determined as approvers, use the **OX** approval procedure.

The approval procedure determines the owner (application role) of an object specified in a request parameter to be the approver. The application role is assigned to the object through a foreign key column. The name of the request parameter is given on the approval step and the name of the table column that references the application role. The approval procedure can be used for all products that are assigned a request property that uses this request parameter.

To use the OX approval procedure

1. Create a multi requestable/unsubscribable resource for use in the IT Shop.
2. Create a service item for this resource and assign a request property to it.
3. Define the request parameters for this request property. At least one parameter must have the following settings:
    - **Parameter name**: Name of the parameter
    - **Data source**: Table
    - **Table column (value query)**: Object key (`XObjectKey`) of the table containing the requested objects.
4. Create an approval workflow with an approval step that uses the OX approval procedure.
    - **Parameter name**: Parameter name of the previously defined request parameter.

- **Column name**: Name of the column that refers to the application role from the table selected in the request parameter.

5. Create an approval policy and assign it to the approval workflow.
6. Assign this approval policy to the service item.

Example: Requesting Microsoft Entra ID role eligibilities

Managers can request Microsoft Entra ID role eligibilities for their employees. When making a request, the specific Microsoft Entra ID role is given as request parameter. Members of the application role assigned to this role as owners are determined as approvers.

One Identity Manager provides the following objects for such requests as default:

- A multi requestable/unsubscribable resource: **Microsoft Entra ID role eligibility**
- A service item for this resource to which the **Microsoft Entra ID role eligibility** request property is assigned
- The **AADRole** request parameter (Microsoft Entra ID role) with the **`AADRole - XObjectKey`** column.
- The **Approval of Microsoft Entra ID role eligibility requests** approval policy
- The **Approval of Microsoft Entra ID role eligibilities** approval workflow with the **Owner of Microsoft Entra ID role** approval step
- Approval step properties
  - Approval procedure: **`OX`**
  - Parameter name: **`AADRole`**
  - Column name: **`UID_AERoleOwner`**

The OX approval procedure determines all members of the application role entered in the `UID_AERoleOwner` column for the Microsoft Entra ID role given in the request.

Related topics

- Default approval procedures on page 105

Determining special approvers

Special approvers are assigned to various objects in One Identity Manager. Different approval procedures can be used to determine these special approvers as approvers.

DR - Role approvers of the department given in the request

A department is entered in the request. An application role for role approvers is assigned to the department `Department.UID_RulerContainer`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

DI - Role approvers (IT) of the department given in the request

A department is entered in the request. An application role for role approvers (IT) is assigned to the department `Department.UID_RulerContainerIT`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

PR - Role approvers of the cost center given in the request

A cost center is entered in the request. An application role for role approvers is assigned to the cost center `ProfitCenter.UID_RulerContainer`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

PI - Role approvers (IT) of the cost center given in the request

A cost center is entered in the request. An application role for role approvers (IT) is assigned to the cost center `ProfitCenter.UID_RulerContainerIT`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

RD - Role approvers of the recipient's primary department

The request recipient is assigned a primary department. An application role for role approvers is assigned to the department `Department.UID_RulerContainer`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

RL - Role approvers of the recipient's primary location

The request recipient is assigned a primary location. An application role for role approvers is assigned to the location `Locality.UID_RulerContainer`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

RO - Role approvers of the recipient's primary business role

Installed modules: Business Roles Module

The request recipient is assigned a primary business role. An application role for role approvers is assigned to the business role `Org.UID_RulerContainer`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

RP - Role approvers of the recipient's primary cost center

The request recipient is assigned a primary cost center. An application role for role approvers is assigned to the cost center `ProfitCenter.UID_RulerContainer`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

ID - Role approvers (IT) of recipient's department

The request recipient is assigned a primary department. An application role for role approvers (IT) is assigned to the department `Department.UID_RulerContainerIT`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

IL - Role approvers (IT) of recipient's location

The request recipient is assigned a primary location. An application role for role approvers (IT) is assigned to the location `Locality.UID_RulerContainerIT`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

IO - Role approvers (IT) of the recipient's primary business role

Installed modules: Business Roles Module

The request recipient is assigned a primary business role. An application role for role approvers (IT) is assigned to the business role `Org.UID_RulerContainerIT`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

IP - Role approvers (IT) of recipient's cost center

The request recipient is assigned a primary cost center. An application role for role approvers (IT) is assigned to the cost center `ProfitCenter.UID_RulerContainerIT`. All secondary members of this application are determined as approvers.

Approvers are determined following the same method as described in Determining approvers via approval roles on page 116.

BE - Approver of the application entitlement

Installed modules: Application Governance Module

Effective when requesting: Application entitlements

The application under which the requested application entitlement is published, is assigned an application role for approvers (`AOBApplication` table, `UID_AERoleApprover` column). All secondary members of this application are determined as approvers. The approvers must be assigned to the **Identity Management | Approvers** application role or a child application role.

If additional approvers (`AOBEntitlement` table, `ObjectKeyAdditionalApprover` column) are assigned to the requested application entitlement, the members of the assigned application role or business role are also determined as approvers.

For more information about applications and application entitlements, see the *One Identity Manager Application Governance User Guide*.

OT - Attestor of the service item to assign

The service item of the requested product is assigned an application role for attestors (`AccProduct` table, `UID_OrgAttestator` column). All secondary members of this application are determined as approvers.

OC - Exception approvers for violated rules

The approval workflow contains a compliance check with the **CR** approval procedure. The compliance rule is assigned an application role for exception approvers. All secondary members of this application are determined as approvers. Exception approvers must be assigned to the **Identity & Access Governance | Identity Audit | Exception approvers** application role or a child application role.

After compliance checking a request, the **OC** approval procedure determines the exception approvers of the violated compliance rules. They decide whether the request is granted approval nevertheless. As it is possible to violate several rules with one request, the request is presented to all the exception approvers in parallel. If one of the exception approvers rejects the exception, the request is rejected.

For more information, see Determining exception approvers on page 136.

OH - Exception approver for worst rule violation

The approval workflow contains an approval step with the **CR** approval procedure. The compliance rule is assigned an application role for exception approvers. All secondary members of this application are determined as approvers. Exception approvers must be assigned to the **Identity & Access Governance | Identity Audit | Exception approvers** application role or a child application role.

After compliance checking a request, the **OC** approval procedure determines the exception approvers of the violated compliance rules. They decide whether the request is granted approval nevertheless. As it is possible to violate several rules with one request, the approval decision is made by the exception approver of the rule that poses the highest threat. In this way, you can accelerate the exception approval procedure for a request that violates several rules.

For more information, see Determining exception approvers on page 136.

Related topics

- Default approval procedures on page 105

Determining approvers via approval roles

The DI, DR, ID, IL, IO, IP, PI, PR, RD, RL, RO, RP approval procedures are used to determine the approvers through the application roles for role approvers and role approvers (IT). These application roles can to assigned to hierarchical roles (departments,

locations, cost centers, business roles). If no application role is assigned to the hierarchical role or this application role has no members, the approvers are determined according to the following principle.

Example: Determine the approvers using the RD approval procedure (Role approvers of the recipient's primary department)

1. This determines the request recipient's primary department (`UID_Department`).
2. The application role (`UID_AERole`) is determined through the department's role approver (`UID_RulerContainer`).
3. Determine the secondary identities assigned to this application role. These can issue approval.
4. If there is no approver given for the primary department or the application role has no members, the approver of the parent department is used.
5. If no approver with members can be determined right up to the top department, the request cannot be decided.

NOTE: When approvers are determined using the approval procedures RO or IO, and inheritance for business roles is defined from the bottom up, the following applies:

If no role approver is given for the primary business role, the role approver is determined from the child business role.

Related topics

- Default approval procedures on page 105
- Determining special approvers on page 113

Determining target system managers as approvers

Every target system connected to a One Identity Manager, can be assigned target system managers. These target system managers can be determined as approvers for requesting system entitlements.

TO - Target system manager of the system entitlement to request

Installed modules: Target System Base Module and other target system modules

Effective when requesting: system entitlements, memberships in system entitlements, assignments of system entitlements to hierarchical roles (assignment requests)

An application role for target system managers (`UID_AERoleOwner` column) is assigned to the target system with the requested system entitlement. All secondary members of this application are determined as approvers. In addition, all members of the parent application roles are determined as approvers Target system managers must be assigned to the **Target systems | <target system>** application role or a child application role.

This finds all target system managers of the system entitlement that are stored as the final product with the request (`PersonWantsOrg.UID_ITShopOrgFinal` column).

Related topics

- Default approval procedures on page 105

Determining requester or recipients

Requesters or recipients of requests sometimes become involved in the approval process. For example, they may have to answer inquiries. The following approval procedures determine the requesters or recipients as approvers.

BR - Back to recipient

Determines the recipient of the request.

Even if the **QER | ITShop | PersonOrderedNoDecide** configuration parameter is set, the recipient can also influence the approval. The approval can be viewed in the approval history. The approval workflow can be continued from any approval level.

BS - Back to requester

Determines the requester.

Even if the **QER | ITShop | PersonInsertedNoDecide** configuration parameter is set, the requester can also influence the approval. The approval can be viewed in the approval history. The approval workflow can be continued from any approval level.

Related topics

- Default approval procedures on page 105
- Approving requests from an approver on page 142

Determining special identities as approvers

Requesters can enter an identity as approver directly into the request. For example, this can be used to assign a manager to the request recipient. This new manager can approve or deny the assignment.

C3 - Identity in additional request data

Prerequisite: Requesters can enter additional request information (`PersonWantsOrg` table, `OrderDetail1` column).

The identity specified in the additional request information is determined as approver.

Related topics

- Default approval procedures on page 105

Automatic approvals

One Identity Manager supports approval of requests with various types of automatic approvals.

CD - Calculated approval

The approval step is approved automatically based on a predefined condition. If the condition returns a result, the approval step is granted approval. If the condition does not return a result, the approval step is denied approval.

For more information, see Calculated approval on page 122.

CR - Compliance check (simplified)

Checks the request for possible rule violations before approval. It takes into account the requested product, all pending requests, and all the company resources already assigned to the request recipient. The approval procedure checks whether the recipient violates existing compliance rules if the requests are granted approval.

Compliance checking requests does not necessarily detect all rule violations. Therefore, it does not replace the cyclical testing of compliance rules.

For more information, see Compliance checking requests on page 134.

EX - Approvals to be made externally

Approval of the approval step is automatically decided as soon as a condition outside the One Identity Manager is fulfilled.

Specify an event in the approval step that triggers an external approval. The event triggers a process initiating external approval for the request and evaluates the result of the approval decision. The approval process waits until the result of the external approval is passed on to One Identity Manager.

For more information, see Approvals to be made externally on page 123.

RI - Identity's risk index

The approval step is automatically approved if the requested product falls below a fixed risk index value.

Prerequisite: The permitted value for the risk index is given in the approval step.

Finds the risk index of the requested product and compares it with the permitted value specified in the approval step. If the risk index is lower than the permitted value the approval step is granted approval. Otherwise, the approval step is not granted approval.

Only risk indexes with inputted values are considered for the approval decision; calculated risk indexes are not taken into account.

For more information, see Request risk analysis on page 132.

SB - Self service

Approval procedure to approve requests automatically. You do not have to specify approvers.

Always define an approval workflow with the **SB** approval procedure as a one-step workflow. That means you cannot set up more approval steps in addition to a self-service

approval step. For more information, see Rule checking for requests with self-service on page 142.

The approval workflow and the **Self service** approval policy are available in the default installation and assigned to the **Identity & Access Lifecycle** shop.

WC - Waiting for further approval

The approval step defers approval until a defined condition is fulfilled. For example, system entitlement requests can be checked and maintained until the corresponding user account is available.

Prerequisite: The condition is defined as a function call in the approval step.

For more information, see Waiting for further approval on page 120.

Related topics

- Default approval procedures on page 105

Waiting for further approval

NOTE: Only one approval step can be defined with the WC approval procedure per approval level.

Use the WC approval procedure within an approval process to ensure that a defined prerequisite is fulfilled before the request is approved. Therefore, approval of a system entitlement request is only possible if existence of the corresponding user account is verified. Deferred approval is useful when a request should be tested for rule conformity. If the user account does not exist when the requested permissions groups are tested, any rule violations that may occur due to the request will not be logged.

You can specify which prerequisites have to be fulfilled so that a request can be presented for approval by defining an appropriate condition. The condition is evaluated as a function call. The function must accept the request UID as a parameter (`PersonWantsOrg.UID_PersonWantsOrg`). It must define three return values as integer values. One of the following actions is carried out depending on the function's return value.

Table 30: Return value for deferred approval

Return value	Action
Return value > 0	The condition is fulfilled. Deferred approval has completed successfully. The next approval step (in case of success) is carried out.
Return value = 0	The condition is not yet fulfilled. Approval is rolled back and is retested the next time DBQueue Processor runs.
Return value < 0	The condition is not fulfilled. Deferred approval has failed. The next approval step (in case of failure) is carried out.

To use an approval procedure

1. Create a database function which tests the condition for the request.
2. Create an approval step with the WC approval procedure. Enter the function call in **Condition**.

   Syntax: `dbo.<function name>`
3. Specify an approval step in the case of success. Use an approval procedure with which One Identity Manager can determine the approvers.
4. Specify an approval step in the case of failure.

Example

To check whether the necessary user account exists when the permissions group is requested, you can use the `TSB_FGIPWODecisionForGroup` function that is supplied.

Table 31: Example of an approval step with deferred approval

Single step:	Waiting Condition
Approval procedures:	WC - Waiting for further approval
Condition:	dbo.TSB_FGIPWODecisionForGroup
Number of approvers:	1

Table 32: Return value for deferred approval decisions in the `TSB_FGIPWODecisionForGroup` function

Return value	Action
Return value > 0	The user account exists, thus fulfilling the condition. The delayed approval is decided positively. The request is passed onto the next approval step. Now an approval step must follow which can establish the approvers for the request.
Return value = 0	The condition is not fulfilled. There is a request pending for a user account or the identity has an account definition with which a user account could be created. Approval is, therefore, deferred, and tested again on the next DBQueue Processor run.
Return value < 0	The condition is not fulfilled. There is no request for a user account and the identity does not have an account definition with which a user account could be created. The delayed approval is decided negatively. The request is passed onto the next approval step.

Related topics

- Default approval procedures on page 105

Calculated approval

NOTE: Only one approval step can be defined with the CD approval procedure per approval level.

It is possible to determine who should be presented with the request for approval on the basis of a defined condition. For example, if the price of the request is below a defined limit, then the department manager can grant approval. If this limit is exceeded, the request has to be presented to the cost center manager. In another case, requests from members of department XY can be granted immediate approval as long as the request does not exceed the defined price limit. If the limit is exceeded or if the employee belongs to another department, the approval has to be granted by the department manager.

To calculate an approval (CD approval procedure), enter a condition when you set up the approval step. If the condition returns a result, the approval step is approved through One Identity Manager. If the condition does not return a result, the approval step is denied by One Identity Manager. If there are no subsequent steps to be carried out, the request is finally granted or denied approval. The condition is defined as a valid where clause for database queries. You can enter the SQL query directly or with a wizard. The condition is always checked for the current request and requester.

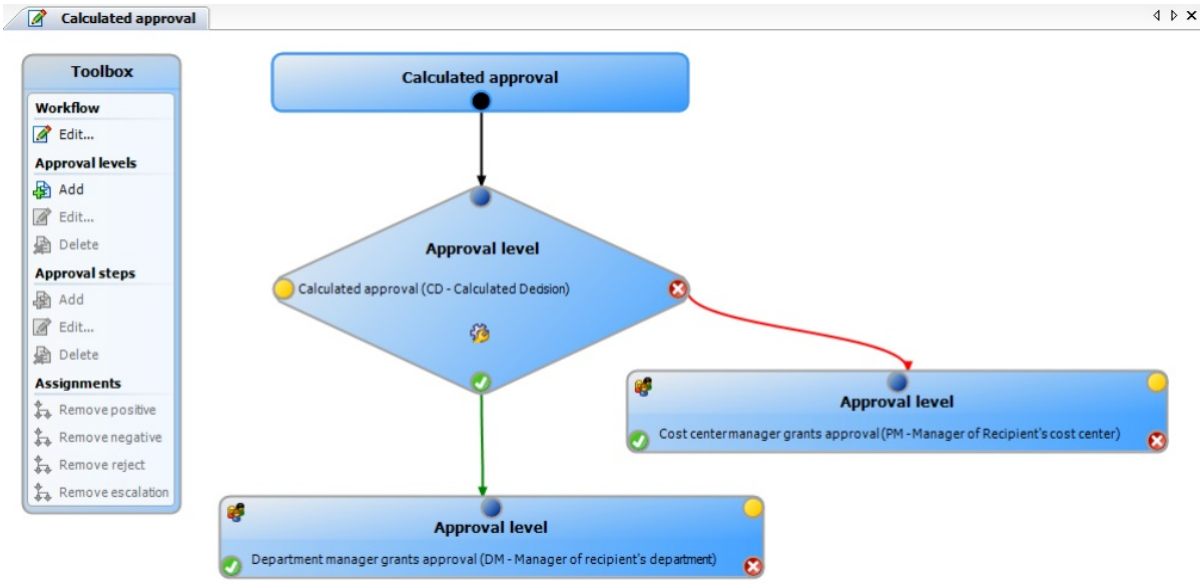
Example for calculated approval

Requests with a price of under 1000 euros can be approved by the customer's department manager. Requests over 1000 euros must be presented to the cost center manager.

Table 33: Approval step with calculated approval

Single step:	Calculated approval
Approval procedures:	CD - Calculated approval
Condition:	`EXISTS (SELECT 1 FROM (SELECT UID_ITShopOrg FROM ITShopOrg WHERE EXISTS (SELECT 1 FROM (SELECT UID_AccProduct FROM AccProduct WHERE round (PurchasePrice, 13) < round(1.000000E+003, 13)) as X WHERE X.UID_AccProduct = ITShopOrg.UID_AccProduct)) as X WHERE X.UID_ITShopOrg = PersonWant-sOrg.UID_Org)`
Number of approvers:	1

Figure 6: Approval workflow showing calculated approval



Related topics

- Default approval procedures on page 105

Approvals to be made externally

Use external approvals (EX approval procedure) if a request needs to be approved once a defined event from outside One Identity Manager takes place. You can also use this procedure to allow users with no access to One Identity Manager to approve requests.

Specify an event in the approval step that triggers an external approval. The event triggers a process that initiates the external approval for the request and evaluates the result of the approval decision. The approval process waits for the external decision to be passed to One Identity Manager. Define the subsequent approval steps depending on the result of the external approval.

To use an approval procedure

1. In the Designer, define your own processes that:
   - Triggers an external approval.
   - Analyzes the results of the external approval.
   - Grants or denies approval in the subsequent external approval step in One Identity Manager.
2. Defines an event that starts the process for external approval. Enter the result in **Result** in the approval step.

If the external event occurs, the approval step status in One Identity Manager must be changed. Use the `CallMethod` process task with the `MakeDecision` method for this. Pass the following parameters to the process task:

```
MethodName: Value = "MakeDecision"

ObjectType: Value = "PersonWantsOrg"

Param1: Value = "sa"

Param2: Value = <approval> ("true" = granted; "false" = denied)

Param3: Value = <reason for approval decision>

Param4: Value = <standard reason>

Param5: Value = <number approval steps> (PWODecisionStep.SubLevelNumber)

WhereClause: Value = "UID_PersonWantsOrg ='"& $UID_PersonWantsOrg$ &"'"
```

Use these parameters to specify which request is to be approved by external approval (`WhereClause`). `Param1` specifies the approver. The approver is always the **sa** system user. `Param2` passes down the approval decision. If the request was granted, a value of **`True`** must be returned. If the request was denied, a value of **`False`** must be returned. Use `Param3` to pass a reason text for the approval decision; use `Param4` to pass a predefined standard reason. If more than one external approval steps have been defined in an approval level, use `Param5` to pass the approval step count. This ensures the approval is aligned with the correct approval step.

Example

All approved requests should be entered into an external ticketing system and started. If a request is completed in an external ticketing system, it must also be completed in One Identity Manager. Use this approval procedure to make external approvals and define:

- A P1 process that creates a ticket with the information about the requested product in the external system and passes the ticket number to One Identity Manager in the request instance.
- An E1 event that starts the P1 event.
- A P2 process that checks whether the ticket status is "closed" and calls the `CallMethod` process task with the `MakeDecision` method in One Identity Manager.
- An E2 event that starts the P2 process.
- A schedule that starts the E2 event on a regular basis.

Enter E1 in the **Event** box as the trigger for the external decision.

Pass the product and customer data that the product is being requested for in the P1 process to the external ticket system. In another parameter, pass the ticket number from the external ticketing system to One Identity Manager.

Use the ticket number to check the ticket status in P2 process. If the ticket is closed, call the `MakeDecision` method and pass the ticket status from the external system to One Identity Manager in a parameter (`Param2`). In another parameter, specify the system user that changes the approval step status in One Identity Manager (`Param1`). Pass **sa** as the value for this parameter. Pass the reason for the approval decision in `Param3`.

For more information about defining processes, see *One Identity Manager Configuration Guide*.

Related topics

- Properties of an approval step on page 95
- Default approval procedures on page 105

Setting up approval procedures

You can create your own approval procedures if the default approval procedures for finding the responsible approvers do not meet your requirements. The condition used to determine the approvers is formulated as a database query. Several queries may be combined into one condition.

To set up an approval procedure

1. In the Manager, select the **IT Shop > Basic configuration data > Approval procedures** category.
2. Click in the result list.
3. Edit the approval procedure main data.
4. Save the changes.

To edit an approval procedure

1. In the Manager, select the **IT Shop > Basic configuration data > Approval procedures > Predefined** category.
2. Select an approval procedure from the result list and run the **Change main data** task.
3. Edit the approval procedure main data.
4. Save the changes.

To edit the condition

1. In the Manager, select the **IT Shop > Basic configuration data > Approval procedures > Predefined** category.
2. Select an approval procedure from the result list.
3. Select **Change queries for approver selection**.

Detailed information about this topic

- General main data of an approval procedure on page 126
- Queries for determining approver on page 126

General main data of an approval procedure

Enter the following main data of an approval procedure.

Table 34: General main data of an approval procedure

Property	Description
Approval procedure	Descriptor for the approval procedure (maximum two characters).
Short description	Short phrase to describe the approval procedure.
DBQueue Processor task	Approvals can either be made automatically through a DBQueue Processor calculation task or by specified approvers. Assign a custom DBQueue Processor task if the approval procedure should make an automatic approval decision. You cannot assign a DBQueue Processor task if there is a query pending to determine approvers.
Max. approvers	Maximum number of approvers to be determined by the approval procedure. Specify how many identities must really make approval decisions in the approval steps used by this approval procedure.
Sort order	Value for sorting approval procedures in the drop-down. • Specify the value **10** to display this approval procedure at the top of the drop-down when you set up an approval step. • To hide the approval procedure in the drop-down, define a negative value. These approval procedures are displayed in the Manager under the **Hidden in Workflow Editor** filter. TIP: It is also possible to change the order for default approval procedures. Move more frequently used approval procedures to the top; hide unused approval procedures.
Description	Detailed description of the approval procedure.

Related topics

- Properties of an approval step on page 95
- Setting up approval procedures on page 125
- Default approval procedures on page 105

Queries for determining approver

The condition used to determine the approvers is formulated as a database query. Several queries may be combined into one condition. This adds all identities determined by single queries to the group of approvers.

To edit the condition

1. In the Manager, select the **IT Shop > Basic configuration data > Approval procedures > Predefined** category.
2. Select an approval procedure from the result list.
3. Select **Change queries for approver selection**.

To create single queries

1. Click **Add**.

   This inserts a new row in the table.
2. Mark this row. Enter the query properties.
3. Add more queries if required.
4. Save the changes.

To edit a single query

1. Select the query you want to edit in the table. Edit the query's properties.
2. Save the changes.

To remove single queries

1. Select the query you want to remove in the table.
2. Click **Delete**.
3. Save the changes.

Table 35: Query properties

Property	Description
Approver selection	Query identifier that determines the approvers.
Query	Database query for determining the approvers. The database query must be formulated as a select statement. The column selected by the database query must return a `UID_Person`. Every query must return a value for `UID_PWORulerOrigin`. The query returns one or more identities to whom the request is presented for approval. If the query fails to a result, the request is canceled. A query contains exactly one select statement. To combine several select statements, create several queries. If a DBQueue Processor task is assigned, you cannot enter a query to determine approvers.
Query for recalculating	Database query for finding request procedures that require recalculation of their approvers.

You can, for example, determine predefined approvers with the query (example 1). The approver can also be found dynamically depending on the request to approve. To do this, access the request to be approved within the database query using the `@UID_PersonWantsOrg` variable (example 2).

Example 1

Requests should be approved by a specific approver.

Query:

```
select UID_Person, null as UID_PWORulerOrigin from Person where InternalName='User, JB'
```

Example 2

Approval for requests should be granted or denied through the requester's parent department. The approver is the cost center manager that is assigned to the requester's primary department. The requester is the identity that triggers a request (`UID_PersonInserted` when requesting for an employee, for example).

Query:

```
select pc.UID_PersonHead as UID_Person, null as UID_PWORulerOrigin from PersonWantsOrg
pwo
    join Person p on pwo.UID_PersonInserted = p.UID_Person
    join Department d on p.UID_Department = d.UID_Department
    join ProfitCenter pc on d.UID_ProfitCenter = pc.UID_ProfitCenter
    where pwo.UID_PersonWantsOrg = @UID_PersonWantsOrg
```

Taking delegation into account

To include delegation when determining approvers, use the query to also determine the identities to whom a responsibility has been delegated. If the managers of hierarchical roles are to make the approval decision, determine the attestors from the `HelperHeadOrg` table. This table groups together all managers, deputy managers, and all other hierarchical role managers as well as their deputies and the identities to whom a responsibility has been delegated.

If the members of business or application roles are to make the approval decision, determine the approvers from the `PersonInBaseTree` table. This table groups together all hierarchical role members and identities to whom a responsibility has been delegated.

To exclude deactivated identities, check the `XOrigin` column for a value greater than **0**. For more information about values in the `XOrigin` column, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To notify the delegator when the delegation recipient has made an approval decision about a request, determine the `UID_PWORulerOrigin`. This also shows in the Web Portal whether the approver originates from a delegation.

To determine the UID_PWORulerOrigin of the delegation

- Determine the UID_PersonWantsOrg of the delegation and copy this value as UID_PWORulerOrigin to the query. Use the dbo.QER_FGIPWORulerOrigin table function to do this.

```
select dbo.QER_FGIPWORulerOrigin(XObjectKey) as UID_PWORulerOrigin
```

To include all active managers and their deputies

- Check the XOrigin column for a value greater than **0**.

Modified query from example 2:

```
select hho.UID_PersonHead as UID_Person, dbo.QER_FGIPWORulerOrigin(hho.XObjectkey) as
UID_PWORulerOrigin from PersonWantsOrg pwo
    join Person p on pwo.UID_PersonInserted = p.UID_Person
    join Department d on p.UID_Department = d.UID_Department
    join ProfitCenter pc on d.UID_ProfitCenter = pc.UID_ProfitCenter
    join HelperHeadOrg hho on hho.UID_Org = pc.UID_ProfitCenter
        and hho.XOrigin > 0
    where pwo.UID_PersonWantsOrg = @UID_PersonWantsOrg
```

Related topics

- Properties of an approval step on page 95
- Setting up approval procedures on page 125
- Default approval procedures on page 105
- Delegations on page 71

Copying an approval procedure

You can copy default approval procedures in order to customize them.

To copy an approval procedure

1. In the Manager, select the **IT Shop > Basic configuration data > Approval procedures** category.
2. Select an approval procedure in the result list. Select the **Change main data** task.
3. Select the **Create copy** task.
4. Confirm the security prompt with **Yes**.
5. Enter the short name for the copy.

   The short name for an approval procedure consists of a maximum of two characters.
6. Click **OK** to start copying.

- OR -

Click **Cancel** to cancel copying.

Deleting approval procedures

To delete an approval procedure

1. Remove all assignments to approval steps.
    a. On the approval procedure overview form, check which approval steps are assigned to the approval procedure.
    b. Switch to the approval workflow and assign another approval procedure to the approval step.
2. In the Manager, select the **IT Shop > Basic configuration data > Approval procedures > Predefined** category.
3. Select an approval procedure from the result list.
4. Click .
5. Confirm the security prompt with **Yes**.

Determining the responsible approvers

The DBQueue Processor calculates which identity is authorized as an approver and in which approval level. Once a request is triggered, the approvers are determined for every approval step of the approval workflow to be processed. Changes to responsibilities may lead to an identity no longer being authorized as an approver for a request that is not yet finally approved. In this case, approvers must be recalculated. The following changes can trigger a recalculation for as yet unapproved requests:

- Approval policy, workflow, step, or procedure changes.
- An authorized approver loses their responsibility in One Identity Manager, for example, if a change is made to the department manager, product owner, or target system manager.
- An identity obtains responsibilities in One Identity Manager and therefore is authorized as an approver, for example as the manager of the request recipient.
- An identity authorized as an approver is deactivated.

Once an identity's responsibilities have changed in One Identity Manager, an approver recalculation task is queued in the DBQueue. By default, all approval steps of the pending approval processes are recalculated at the same time. Approval steps that have already been approved remain approved, even if their approver has changed. Recalculating approvers may take a long time depending on the configuration of the system environment and the amount of data to be processed. To optimize this processing time, you can specify the approval steps for which the approvers are to be recalculated.

NOTE: The approver recalculation task is set for approval steps that implement default approval procedures. Approval steps with customized approval procedures are not recalculated automatically.

To configure recalculation of approvers

- In the Designer, set the **QER | ITShop | ReducedApproverCalculation** configuration parameter and select one of the following options as the value.

Table 36: Options for recalculating approvers

Option	Description
No	All approval steps are recalculated. This behavior also applies if the configuration parameter is not set. Advantage: All valid approvers are displayed in the approval process. The rest of the approval sequence is transparent. Disadvantage: Recalculating approvers may take a long time.
CurrentLevel	Only approvers for the approval level that is currently to be edited are recalculated. Once an approval level has been approved, the approvers are determined for the next approval level. Advantage: The number of approval levels to calculate is lower. Calculating the approvers may be faster. TIP: Use this option if performance problems occur in your environment in connection with the recalculation of approvers. Disadvantage: The originally calculated approvers are still displayed in the approval sequence for each subsequent approval step, even though they may no longer have approval authorization. The rest of the approval sequence is not correctly represented.
NoRecalc	No recalculation of approvers The previous approvers remain authorized to approve the current approval levels. Once an approval level has been approved, the approvers are determined for the next approval level. Advantage: The number of approval levels to calculate is lower. Calculating the approvers may be faster. TIP:Use this option if performance problems occur in your environment in connection with the recalculation of approvers, even though the **`CurrentLevel`** option is used. Disadvantage: The originally calculated approvers are still displayed in the approval sequence for each subsequent approval step, even though they may no longer have approval authorization. The rest of the approval sequence is not correctly represented. Identities that are no longer authorized can approve

Option	Description
	the current approval level. In the worst-case scenario, the only attestors originally calculated here now have no access to One Identity Manager, for example, because they have left the company. The approval level cannot be approved. ***To see approval steps of this type through*** • Define a timeout and timeout behavior when you set up the approval workflows on the approval steps. - OR - • When setting up the IT Shop, assign members to the chief approval team. These can access open approval processes at any time.

Detailed information about this topic

- Properties of an approval step on page 95
- Chief approval team on page 215

Related topics

- Changing approval workflows of pending requests on page 176

Request risk analysis

Everyone with IT system authorization in a company represents a security risk for that company. For example, an identity with permission to edit financial data in SAP carries a higher risk than an identity with permission to edit their own main data. To quantify the risk, you can enter a risk value for every company resource in One Identity Manager. A risk index is calculated from this value for every identity that has this company resource assigned to it directly or indirectly. Company resources include target system entitlements (for example, Active Directory groups or SAP profiles), system roles, subscribable reports, software, and resources. In this way, all the people that represent a particular risk to the company can be found.

Every time a company resource with a specified risk index is assigned, the identity's risk index may exceed a permitted level. You can check the risk index of company resources if they are requested through the IT Shop. If the risk index is higher than the specified value, the request is denied.

To set up risk assessment for requests

- Create an approval workflow.
    1. Add an approval step with the RI approval procedure.
    2. In the **Condition** field, enter the comparison value for the risk index. Enter a number in the range `0.0 to 1.0`.
    3. Enter other approval levels if required.

The approval step is granted approval by One Identity Manager if the risk index of the requested company resource is lower than the comparison value. If the risk index is higher or equal to the comparison value, the approval step is not granted approval.

Risk assessment of requests works for both direct company resource request and assignment requests. Only risk indexes with inputted values are examined for the approval decision; calculated risk indexes are not taken into account. Therefore, risk assessment of requests only works if the product's original table or one of the member tables of a requested assignment has a `RiskIndex` column. If the table only has the `RiskIndexCalculated` column, the request is automatically approved. If both member tables of an assignment request have a `RiskIndex` column, the highest of the two risk indexes is used as the basis for the approval.

If the company resource request or an assignment has been granted approval, the identity's risk index is recalculated the next time the scheduled calculation task is run.

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

Related topics

- Properties of an approval step on page 95

Testing requests for rule compliance

Installed modules: Compliance Rules Module

You can integrate rule conformity testing for IT Shop requests within an approval workflow. A separate approval procedure is supplied for this. This approval procedure checks whether the request's recipient will violate compliance rules if the requests are granted approval. The result of the test is logged in the request's approval sequence and approval history.

Table 37: Approval procedures for compliance checking

Approval procedure	Description
CR - compliance check (simplified)	Checks the current request for possible rule violations. It takes into account the requested product and all the company resources already assigned to the request recipient.

Prerequisites for request validation

- Compliance rules are defined.

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

- The approval workflow contains an approval step with the CR approval procedure.

  For more information, see Compliance checking requests on page 134.

Compliance checking requests

To retain an overview of potential rule violations, you can run a simplified compliance check. Use the CR approval procedure to test requests for possible rule violations before finally approving them.

The following data of a recipient's request is taken into account by the compliance check:

- All pending requests
- All company resources already assigned to the recipient
- All the recipient's user accounts
- All entitlement in the target system (for example, Active Directory groups or SAP roles) the recipient has obtained through these user accounts

Auxiliary tables for object assignments are regularly evaluated for the compliance check. Auxiliary tables are calculated on a scheduled basis. Furthermore, the approval procedure only takes into account compliance rules that are created using the simplified definition.

Rule checking does not completely check the requests with this. It is possible that under the following conditions, rule checking does not identify a rule violation:

- Customer permissions change after the auxiliary table have been calculated.
- If memberships are requested in business role or organization, a rule is violated by an object that is inherited through the business role or organization. Inheritance is calculated after request approval and can therefore not be identified until after the auxiliary table is calculated again.
- The customer does not belong to the identities affected by a rule until the request is made.
- The rule condition was created in expert node or as an SQL query.

TIP: A complete check of assignments is achieved with cyclical testing of compliance rule using schedules. This finds all the rule violations that result from the request.

It is possible that under the following conditions, rule checking identifies a rule violation where one does not exist:

- Two products violate one rule when they are assigned at the same time. The product requests are, however, for a limited period. The validity periods does not overlap. Still a potential rule violation is identified.

TIP: These requests can be approved after checking by exception approver as permitted by the definition of the violation rule.

The compliance check is not only useful for specifying which rule is violated by a request, but it can also find out which product in the request caused the rule violation. This makes a detailed analysis possible of the rule violation. The request can still be approved by exception approval, the definition of compliance rules permitting. Additional approval steps are added in approval workflows to deal with exception approval.

Conditions for compliance checking requests

- You can add only one approval step per approval policy with the CR approval procedure.
- The rule conditions were created in the simple definition.
- IT Shop properties that are specified for each rule are taken into account in the rule testing. Identification of a rule violation depends on the setting on **Rule violation identified**.
- The compliance check should be added as the last approval level in the approval workflow. The subsequent approval levels only get one approval step to determine the exception approver if approval is denied.

Compliance check sequence

1. If an approval step for compliance checking using the CR approval procedure is found in the request's approval procedure, all products in pending requests are assigned to the customer. It is assumed that all pending requests will be approved and therefore the customer will obtain all the products. The current request is then analyzed with respect to potential violations against the defined rules.
2. If no rule violations are found, the approval step is automatically granted approval and the request is passed on to the approver at the next approval level above.
3. If a rule violation is detected, the request is automatically not granted approval. The request can still be approved by exception approval, the definition of rule violations permitting.

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

Related topics

- Identifying rule violations on page 136
- Determining exception approvers on page 136
- Default approval procedures on page 105

Identifying rule violations

If the **QER | ComplianceCheck | EnableITSettingsForRule** configuration parameter is set, properties can be added to compliance rules that are taken into account when rule checking requests.

Specify which violation should be logged for the rule by using the **Rule violation identified** IT Shop property.

Table 38: Permitted values

Value	Description
New rule violation due to a request	Only rule violations that are added through approval of the current request are logged.
Unapproved exception	Rule violations that are added through approval of the current request are logged. Already known rule violations that have not yet been granted an exception are also logged.
Any compliance violation	All rule violations are logged, independent of whether an exception approval has already been granted or not. This value is automatically set when the **Explicit exception approval** option is set.

If the **QER | ComplianceCheck | EnableITSettingsForRule** configuration parameter is not set, new rule violations are logged through the current request.

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

Determining exception approvers

Requests that may cause a rule violation can still be approved by exception approval.

To allow exception approval for request with rule violations

1. Enable the **Exception approval allowed** option for the compliance rule and assign an exception approver.

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

2. Enter an approval step in the approval workflow with the OC or OH procedure. Connect this approval level with the compliance checking approval level at the connection point for denying this approval decision.

   NOTE:

- Only apply this approval procedure immediately after an approval level with the CR approval procedure.
- For each approval workflow, **only one** approval step can be defined using the OC or OH approval procedure.

3. If the **QER | ComplianceCheck | EnableITSettingsForRule** configuration parameter is set, you can use the rule's IT Shop properties to configure which rule violations are presented to an exception approver. Set or unset **Explicit exception approval** to do this.

   For more information, see Explicit exception approval on page 141.

Table 39: Approval procedures for exception approval

Approval procedure	Description
OC (Exception approvers for violated rules)	The approval decision is agreed on by the exception approvers of the violated rule. As it may be possible that several rule are broken with one request, the request is presented to all the exception approvers in parallel. If one of the exception approvers rejects the exception, the request is rejected.
OH (exception approver for worst rule violation)	The approval decision is agreed on by the rule's exception approver which poses the highest threat. In this way, you can accelerate the exception approval procedure for a request that violates several rules. Ensure the following apply for this approval procedure: • The severity level is set in the assessment criteria for all compliance rules. • The exception approver for the worst rule violation in all affected rules is one of the exception approvers.

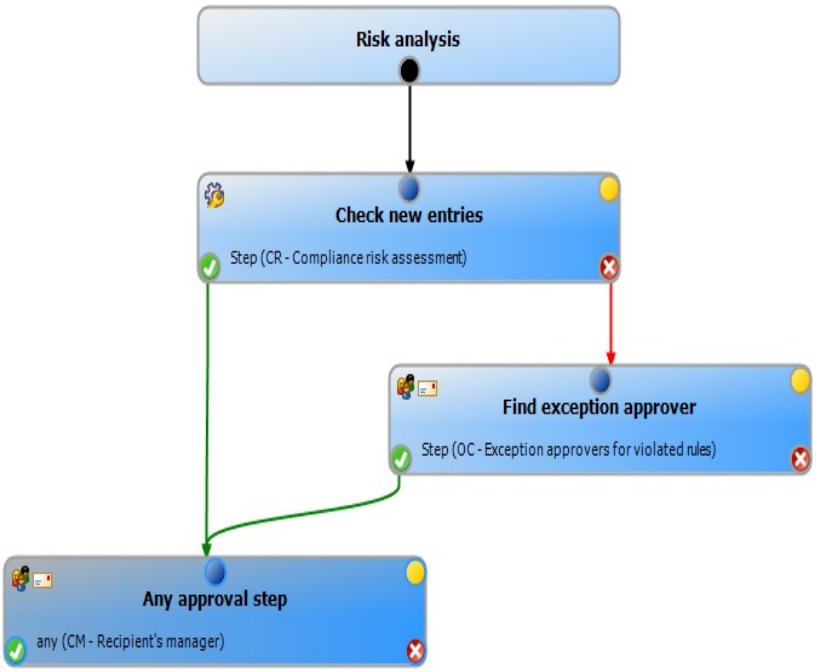
Example

Four different compliance rules are violated by a request for Active Directory group membership. The target system manager of the Active Directory domain is entered as exception approver for all the compliance rules.

Using the OC approval procedure, the target system manger must grant approval exceptions for all four compliance rules.

Using the OH approval procedure, the target system manager is presented with the request only for the compliance rule with the highest severity code. The manager's decision is automatically passed on to the other violated rules.

Figure 7: Example of an approval workflow with compliance checking and exception approval



Sequence of compliance checking with exception approval

1. If a rule violation is detected during compliance checking, the request is automatically not granted approval. The request is passed on to the approver of the next approval level for approval.
2. Exception approvers are found according to the given approval procedure.
3. If exception approval is granted, the request is approved and assigned.
4. If exception approval is not granted, the request is denied.

IMPORTANT: If the **QER | ITShop | ReuseDecision** configuration parameter is set and the exception approver has already approved as the request an approver in a previous approval step, exception approval is automatically granted. For more information, see Automatically approving requests on page 144.

NOTE:

- As opposed to the manager/deputy principle normally in place, an exception approver's deputy is NOT permitted to grant exception approval alone.
- You cannot determine fallback approvers for exception approvers. The request is canceled if no exception approver can be established.
- The chief approval team cannot grant exception approvals.

Restricting exception approvers

By default, exception approvers can also make approval decisions about requests in which they are themselves requester (`UID_PersonInserted`) or recipient (`UID_PersonOrdered`). To prevent this, you can specify the desired behavior in the following configuration parameter and in the approval step:

- **QER | ComplianceCheck | DisableSelfExceptionGranting** configuration parameter
- **QER | ITShop | PersonOrderedNoDecideCompliance** configuration parameter
- **QER | ITShop | PersonInsertedNoDecideCompliance** configuration parameter
- **Approval by affected identity** option in the approval step for finding exception approvers

If the requester or approver is not allowed to grant approval exceptions, their main identity and all sub identities are removed from the circle of exception approvers.

Summary of configuration options

Requesters can grant exception approval for their own requests, if:

- **PersonInsertedNoDecideCompliance** configuration parameter is not set.

  - OR -

- **Approval by affected identity** option is set.

Recipients can grant exception approval for their own requests, if:

- **DisableSelfExceptionGranting** configuration parameter is not set.

  PersonOrderedNoDecideCompliance configuration parameter is not set.

  - OR -

- **DisableSelfExceptionGranting** configuration parameter is not set.

  Approval by affected identity option is set.

Requesters cannot grant exception approval, if:

- **PersonInsertedNoDecideCompliance** configuration parameter is set.

  Approval by affected identity option is not set.

Recipients cannot grant exception approval, if:

- **DisableSelfExceptionGranting** configuration parameter is set.

  - OR -

- **PersonOrderedNoDecideCompliance** configuration parameter is set.

  Approval by affected identity option is not set.

Related topics

- Setting up exception approver restrictions on page 140
- Approving requests from an approver on page 142

Setting up exception approver restrictions

To prevent recipients of request becoming exception approvers

- In the Designer, disable the **QER | ComplianceCheck | DisableSelfExceptionGranting** configuration parameter.

  This configuration parameter takes effect:

  - When requests are granted approval exception.
  - During cyclical rule checking. For more information about cyclical rule checking, see the *One Identity Manager Compliance Rules Administration Guide*.

  - OR -

- In the Designer, enable the **QER | ITShop | PersonOrderedNoDecideCompliance** configuration parameter.

  This configuration parameter takes effect:

  - When requests are granted approval exception.
  - If the **Approval by affected identity** option is disabled in the approval step.

To prevent requesters becoming exception approvers

- In the Designer, set the **QER | ITShop | PersonInsertedNoDecideCompliance** configuration parameter.

  This configuration parameter takes effect:

  - When requests are granted approval exception.
  - If the **Approval by affected identity** option is disabled in the approval step.

For individual approval workflows, you can allow exceptions to the general rule in the **PersonInsertedNoDecide** and **PersonOrderedNoDecide** configuration parameters. Use these options if the requester or recipient of requests is allowed to grant themselves exception approval only for certain requests.

To allow request recipients or requesters to become exception approvers in certain cases

- In the approval step for determining exception approvers, enable the **Approval by affected identity** option.

Related topics

- Properties of an approval step on page 95
- Approving requests from an approver on page 142
- Restricting exception approvers on page 139

Explicit exception approval

If the **QER | ComplianceCheck | EnableITSettingsForRule** configuration parameter is set, properties can be added to compliance rules that are taken into account when rule checking requests.

Use the **Explicit exception approval** IT Shop property to specify whether the reoccurring rule violation should be presented for exception approval or whether an existing exception approval can be reused.

Table 40: Permitted values

Option is	Description
Enabled	A known rule violation must always be presented for exception approval, even if there is an exception approval from a previous violation of the rule.
Not set	A known rule violation is not presented again for exception approval if there is an exception approval from a previous violation of the rule. This exception approval is reused and the known rule violation is automatically granted exception.

If several rules are violated by a request and **Explicit exception approval** is set for one of the rules, the request is presented for approval to **all** exception approvers for this rule.

Rules that have **Explicit exception approval** set result in a renewed exception approval if:

- A rule check is carried out within the approval process for the current request.

  - AND -

  a. The rule is violated by the current request.

     - OR -

  b. The IT Shop customer has already violated the rule.

In case (a), the request for the IT Shop customer is presented to the exception approver. If the request is approved, case (b) applies to the next request. In case (b), every request for the IT Shop customer must be decided by the violation approver, even when the request itself does not result in a rule violation. The result you achieve is that assignments for identities that have been granted an exception, are verified and reapproved for every new request.

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

Rule checking for requests with self-service

Self-service (SB approval procedure) is always defined as a one-step procedure. That means you cannot set up more approval steps in addition to a self-service approval step.

To realize compliance checking for requests with self-service

- Create an approval workflow with a single approval level. The approval workflow contains an approval step with the CR approval procedure. For more information, see Compliance checking requests on page 134.

  If the rule check is successful, the request is granted approval and self-service is accomplished implicitly.

  To make exception approval possible for rule violations, add an approval level with the OC or OH approval procedure. For more information, see Determining exception approvers on page 136.

Approving requests from an approver

By default, approvers can make approval decisions about requests in which they are themselves requester (`UID_PersonInserted`) or recipient (`UID_PersonOrdered`). To prevent this, you can specify the desired behavior in the following configuration parameter and in the approval step.

- **QER | ITShop | PersonOrderedNoDecide** configuration parameter
- **QER | ITShop | PersonInsertedNoDecide** configuration parameter
- **Approval by affected identity** option in the approval step.

If the requester or approver is not allowed to make approval decisions, their main identity and all subidentities are removed from the group of approvers.

NOTE:

- The configuration parameter setting also applies for fallback approvers; it does not apply to the chief approval team.
- This configuration parameter does not affect the BS and BR approval procedures. These approval procedures also find the requester and the request recipient if the configuration parameter is not set. For more information, see Determining requester or recipients on page 118.

Summary of configuration options

Requesters can approve their own requests if:

- The **PersonInsertedNoDecide** configuration parameter is not set.

  - OR -

- The **Approval by affected identity** option is set.

Recipients can approve their own requests if:

- The **PersonOrderedNoDecide** configuration parameter is not set.

  - OR -

- The **Approval by affected identity** option is set.

Requesters cannot approve if:

- The **PersonInsertedNoDecide** configuration parameter is set.

  The **Approval by affected identity** option is not set.

Recipients cannot approve if:

- The **PersonOrderedNoDecide** configuration parameter is set.

  The **Approval by affected identity** option is not set.

Example

A department manager places a request for an employee. Both of them are found to be approvers by the approval procedure. To prevent the department manager from approving the request, set the **QER | ITShop | PersonInsertedNoDecide** parameter. To prevent the employee from approving the request, set the **QER | ITShop | PersonOrderedNoDecide** parameter.

Approving requests from an exception approver

Similarly, you specify whether exception approvers are allowed to approve their own requests if compliance rules are violated by a request. For more information, see Restricting exception approvers on page 139.

Related topics

- Setting up approver restrictions on page 144
- Automatically approving requests on page 144

Setting up approver restrictions

To prevent recipients of requests becoming approvers

- In the Designer, set the **QER | ITShop | PersonOrderedNoDecide** configuration parameter.

  This configuration parameter takes effect if the **Approval by affected identity** option is not set on the approval step.

To prevent requesters becoming approvers

- In the Designer, set the **QER | ITShop | PersonInsertedNoDecide** configuration parameter.

  This configuration parameter takes effect if the **Approval by affected identity** option is not set on the approval step.

For individual approval workflows, you can allow exceptions to the general rule in the **PersonInsertedNoDecide** and **PersonOrderedNoDecide** configuration parameters. Use these options to allow the requester or recipient of requests to make approval decisions themselves in single approval steps.

To allow request recipients or requesters to become approvers in certain cases

- On the approval step, enable the **Approval by affected identity** option.

Related topics

- Properties of an approval step on page 95
- Approving requests from an approver on page 142

Automatically approving requests

Approvers may be involved in an approval process more than once, for example, if they are also requesters or determined as approvers in various approval steps. In such cases, the approval process can be speeded up with automatic approval.

NOTE: Automatic approvals apply to all fallback approvers but not to the chief approval team.

Use configuration parameters to specify when automatic approvals are used. You can specify exceptions from default behavior for individual approval steps. Specify the behavior you expect in the following configuration parameters and approval steps.

- **QER | ITShop | DecisionOnInsert** configuration parameter
- **QER | ITShop | AutoDecision** configuration parameter

- **QER | ITShop | ReuseDecision** configuration parameter
- **No automatic approval** option in the approval step

Summary of configuration options

Approval steps are automatically approved or denied if:

- The **QER | ITShop | DecisionOnInsert** configuration parameter is set.
  The **No automatic approval** option is not set.
  - OR -
- The **QER | ITShop | AutoDecision** configuration parameter is set.
  The **No automatic approval** option is not set.
  - OR -
- The **QER | ITShop | ReuseDecision** configuration parameter is set.
  The **No automatic approval** option is not set.

Requests are manually approved or denied if:

- The **QER | ITShop | DecisionOnInsert** configuration parameter is not set.
  - OR -
- The **QER | ITShop | AutoDecision** configuration parameter is not set.
  - OR -
- The **QER | ITShop | ReuseDecision** configuration parameter is not set.
  - OR -
- The **No automatic approval** option is set.

Detailed information about this topic

- Configuring automatic approval on page 146

Related topics

- Approval by the chief approval team on page 161
- Approvers cannot be established on page 157
- Timeout on saving requests on page 255
- Approving requests from an approver on page 142

Configuring automatic approval

Scenario: An approver can grant or deny approval in several approval steps.

An approver may be authorized to approve several levels of an approval workflow. By default, the request is presented to the approver in each approval level. You can allow automatic approval so that the approver is not presented with a request more than once.

To allow an approver's decisions to be met automatically in several sequential approval levels

- In the Designer, set the **QER | ITShop | AutoDecision** configuration parameter.

  The approval decision of the first approval levels is applied to subsequent approval levels for which the approver is authorized.

  The configuration parameter takes effect if the **No automatic approval** option is not enabled for the approval step.

To attain automatic acceptance of an approver's approval decisions for subsequent approval levels

- In the Designer, set the **QER | ITShop | ReuseDecision** configuration parameter.

  If the approver granted approval to this request in an earlier approval step, the approval decision is passed on irrespective of how the approval steps in between were approved. If the approver did not grant approval in an earlier approval step, the request is presented for approval again.

  The configuration parameter takes effect if the **No automatic approval** option is not enabled for the approval step.

  IMPORTANT: If the approver is also an exception approver for compliance rule violations, requests that violate compliance rules will also be automatically approved without being presented for exception approval.

Scenario: Requester is also approver

Approvers can run requests for themselves. If a requester is determined to be approver for the request, their approval steps are immediately granted approval.

To prevent automatic approval for an approver's requests

- In the Designer, disable the **QER | ITShop | DecisionOnInsert** configuration parameter.

  If a requester is determined to be the approver of an approval step, the request is presented to the requester to be approved.

The **QER | ITShop | DecisionOnInsert** configuration parameter is set by default and takes effect if the **No automatic approval** option is not enabled in the approval step.

If the **QER | ITShop | PersonInsertedNoDecide** configuration parameter is set, the requester does not become an approver and cannot approve the request. Also, the request cannot be decided automatically.

Preventing automatic approval in individual cases

For single approval steps, you can configure exceptions to the general rule in the configuration parameters.

To prevent automatic approvals for particular approval steps

- Enable the **No automatic approval** option in the approval step.

  The **QER | ITShop | DecisionOnInsert**, **QER | ITShop | ReuseDecision**, and **QER | ITShop | AutoDecision** configuration parameters are not considered in this approval step. In each case, requests are to be presented to the approver of this approval step.

Related topics

- Automatically approving requests on page 144
- Properties of an approval step on page 95
- Approving requests from an approver on page 142
- Determining exception approvers on page 136

Approval by peer group analysis

Using peer group analysis, approval for requests 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. So, if a company resource has already been assigned to a majority of employees in a department, a new request for this company resource is automatically approved. This helps to accelerate approval processes.

Peer group analysis is carried out when requesting single request products as well as multi-request products.

Peer groups contain all identities with the same manager or belonging to the same primary or secondary department as the request's recipient. Configuration parameters specify which identity belong to the peer group. At least one of the following configuration parameters must be set.

- **QER | ITShop | PeerGroupAnalysis | IncludeManager**: Identities that have the same manager as the request's recipient
- **QER | ITShop | PeerGroupAnalysis | IncludePrimaryDepartment**: Identities that belong to the same primary department as the request's recipient

- **QER | ITShop | PeerGroupAnalysis | IncludeSecondaryDepartment**: Identities whose secondary department corresponds to the primary or secondary department of the request's recipient

The proportion of identities of a peer group who must already own the company resource, is set in the **QER | ITShop | PeerGroupAnalysis | ApprovalThreshold** configuration parameter. The threshold specifies the ratio of the total number of identities in the peer group to the number of identities in the peer group who already own this product.

You can also specify that employees are not allowed to request cross-functional products, which means, if the requested product and the primary department of the request recipient are from different functional areas, the request should be denied. To include this check in peer group analysis, set the **QER | ITShop | PeerGroupAnalysis | CheckCrossfunctionalAssignment** configuration parameter.

Requests are automatically approved for fully configured peer group analysis, if both:

- The requested product is not cross-functional
- The number of identities in the peer group who already own this product equals or exceeds the given threshold.

If this is not the case, requests are automatically denied.

To use this functionality, the One Identity Manager provides the `QER_PersonWantsOrg_Peer group analysis` process and the `PeergroupAnalysis` event. The process is run using an approval step with the EX approval procedure.

Detailed information about this topic

- Configuring peer group analysis for requests on page 148

Related topics

- Approval recommendations for requests on page 149

Configuring peer group analysis for requests

To configure peer groups

1. In the Designer, set the **QER | ITShop | PeerGroupAnalysis** configuration parameter.
2. Set at least on of the following subparameters:
    - **QER | ITShop | PeerGroupAnalysis | IncludeManager**: Identities who have the same manager as the request's recipient
    - **QER | ITShop | PeerGroupAnalysis | IncludePrimaryDepartment**: Identities who belong to the same primary department as the request's recipient

- **QER | ITShop | PeerGroupAnalysis | IncludeSecondaryDepartment**: Identities whose secondary department corresponds to the primary or secondary department of the request's recipient

Thus, you specify which identities belong to the peer group. You can also set two or all of the configuration parameters.

3. To specify a threshold for the peer group, set the **QER | ITShop | PeerGroupAnalysis | ApprovalThreshold** configuration parameter and specify a value between **0** and **1**.

   The default value is **0.9**. That means, at least 90 percent of the peer group members must already have the requested product so that the request can be approved.

4. (Optional) To check whether the requested product is cross-functional, enable the **QER | ITShop | PeerGroupAnalysis | CheckCrossfunctionalAssignment** configuration parameter.

   a. Assign the service items and departments to functional areas.

      Only functional areas that are primary assigned service items are taken into account.

      For more information about functional areas, see the *One Identity Manager Identity Management Base Module Administration Guide*.

   b. Assign identities to primary departments.

5. In the Manager, create an approval workflow with at least one approval level. For the approval step, enter at least the following data:

   - Single step: **EXWithPeerGroupAnalysis**.
   - Approval procedure: **EX**
   - Event: **PeerGroupAnalysis**

   The event starts the `QER_PersonWantsOrg_Peer group analysis` process, which runs the `QER_PeerGroupAnalysis` script.

   The script runs automatic approval and sets the approval step type to **Grant** or **Deny**.

Detailed information about this topic

- Approval by peer group analysis on page 147

Related topics

- Approvals to be made externally on page 123
- General main data for service items on page 23

Approval recommendations for requests

A further way to accelerate the approval process by making automatic approval decisions, is with approval recommendations. This uses different criteria to determine whether it is

reasonable to grant or deny approval for a request. A peer group analysis is performed to determine approval recommendations and other criteria are analyzed. Based on the recommendation, requests can be automatically granted approval. If a denying approval is recommended or a clear recommendation cannot be made, the requests must be submitted to additional approvers. These approvers are shown the approval recommendation and the details of the recommendation so that they can use this information to make an approval decision.

Detailed information about this topic

- Criteria for approval recommendations for requests on page 150
- Configuring approval recommendations for requests on page 152
- Approval by peer group analysis on page 147

Criteria for approval recommendations for requests

The following criteria are taken into account when determining recommendations for approving requests.

1. Peer group factor

   The number of identities in a peer group that already own the requested product is determined. If this number exceeds the specified threshold, granting approval is recommended. The threshold is specified in the **QER | ITShop | Recommendation | PeerGroupThreshold** configuration parameter.

   Peer groups contain all identities with the same manager or belonging to the same primary or secondary department as the request's recipient. Configuration parameters specify which identity belong to the peer group. At least one of the following configuration parameters must be set.

   - **QER | ITShop | PeerGroupAnalysis | IncludeManager**: Identities that have the same manager as the request's recipient
   - **QER | ITShop | PeerGroupAnalysis | IncludePrimaryDepartment**: Identities that belong to the same primary department as the request's recipient
   - **QER | ITShop | PeerGroupAnalysis | IncludeSecondaryDepartment**: Identities whose secondary department corresponds to the primary or secondary department of the request's recipient

   Peer group factor is determined when requesting single request products as well as multi-request products.

2. Assigned functional area

   The requested product and the primary department of the request recipient are checked to see if they are assigned to the same functional area.

3. Compliance rule violations

   The request's recipient is checked for violation of current compliance rules if their request is granted approval. Once a rule violation is detected, denying approval is recommended.

4. Risk factor

   The risk factor of the request's recipient is calculated. The risk index of the requested product is already taken into account. If this risk index exceeds the specified threshold, denying approval is recommended. The threshold is specified in the **QER | ITShop | Recommendation | RiskIndexThreshold** configuration parameter.

5. Approval rate

   This determines the proportion of approvals for this product in previous requests. For this, all approval procedures with manual approval that are also used in the currently running approval workflow are determined in the approval sequence (`PWODecisionHistory`). The proportion of approvals for the same product is determined from the entries in the approval sequence.

   If the approval rate exceeds the specified threshold, granting approval is recommended. The threshold is specified in the **QER | ITShop | Recommendation | ApprovalRateThreshold** configuration parameter.

6. Assignment rate

   The number of company resource assignments to the request recipient is determined (`PersonHasObject`) and compared to the average number per identity. If the assignment rate is less that the average per identity, denying approval is recommended.

Recommendation for granting approval

All criteria are fulfilled. That means:

- The peer group has members and the peer group factor is higher than the threshold (**PeerGroupThreshold**).
- Requested product and primary department belong to the same function area. The product is therefore not cross-functional.
- There are not rule violations.
- The risk index of the request recipient is lower than the threshold (**RiskIndexThreshold**).
- The approval rate is higher than the threshold (**ApprovalRateThreshold**).
- The assignment rate is higher than average.

Recommendation for denying approval

At least one of the following criteria applies.

- The peer group has no members or the peer group factor is lower than the threshold (**PeerGroupThreshold**).

- There is at least one rule violation.
- The assignment rate is less than average.

If at least two of the following criteria apply, denying approval is also recommended.

- The product is cross-functional.
- The risk index of the request recipient is higher than the threshold (**RiskIndexThreshold**).
- The approval rate is lower than the threshold (**ApprovalRateThreshold**).

In all other cases, no recommendation is given.

Related topics

- Approval recommendations for requests on page 149
- Configuring approval recommendations for requests on page 152

Configuring approval recommendations for requests

To use approval recommendations, add an additional approval level to the approval workflows and configure the thresholds. Based on the recommendation, requests can be automatically granted approval. If a denying approval is recommended or a clear recommendation cannot be made, the requests must be submitted to additional approvers. If requests are not approved automatically, define a manual approval level in the event that granting approval is recommended.

The approvers are shown the approval recommendation. They can follow the recommendation or make their own approval decision independently.

TIP: For approval recommendations with automatic approval, One Identity Manager provides the sample workflow **Recipient's manager (with approval recommendation)**. You can use this approval workflow as a template and adjust to suit your requirements. To do this, copy the workflow and add approval levels with manual approval steps.

To configure approval recommendations

1. In the Designer, set the **QER | ITShop | PeerGroupAnalysis** configuration parameter.
2. Set at least on of the following subparameters:
    - **QER | ITShop | PeerGroupAnalysis | IncludeManager**: Identities who have the same manager as the request's recipient
    - **QER | ITShop | PeerGroupAnalysis | IncludePrimaryDepartment**: Identities who belong to the same primary department as the request's

recipient

- **QER | ITShop | PeerGroupAnalysis | IncludeSecondaryDepartment**: Identities whose secondary department corresponds to the primary or secondary department of the request's recipient

Thus, you specify which identities belong to the peer group. You can also set two or all of the configuration parameters.

3. Specify the threshold for the peer group factor in the **QER | ITShop | Recommendation | PeerGroupThreshold** configuration parameter. Enter a value between **0** and **1**.

   The default value is **0.9**. That means, at least 90 percent of the peer group members must already have the requested product so that the granting approval can be recommended.

4. Set the threshold for the risk factor in the **QER | ITShop | Recommendation | RiskIndexThreshold** configuration parameter. Enter a value between **0** and **1**.

   The default value is **0.5**. That means, the request recipient's risk index must be less than 0.5 for granting approval to be recommended.

5. Set the approval rate threshold in the **QER | ITShop | Recommendation | ApprovalRateThreshold** configuration parameter. Enter a value between **0** and **1**.

   The default value is **0.5**. That means, if more than 50% of all previous requests of this product were approved using the same approval procedure, granting approval is recommended.

6. Create an approval workflow in the Manager and insert an approval step with the following data as the first approval level:

   - Approval procedure: **EX**
   - Event: **RecommendationAnalysis**

   The event starts the `QER_PersonWantsOrg_Recommendation` process, which runs the `QER_PersonWantsOrg_Recommendation` script. The script runs automatic approval.

7. Add an approval level to manual approval.
8. In case denying approval might be recommended or no recommendation can be made, connect this approval level to the deny connection point at the first approval level.
9. (Optional) If the request is not to be approved automatically, connect the connection point for granting approval at the first approval level to an approval level for manual approval as well. This means that requests have to be approved manually even if granting approval is recommended.
10. Create an approval policy and assign it to the approval workflow.

    - Use this approval policy in the IT Shop.

Related topics

- Approval recommendations for requests on page 149
- Criteria for approval recommendations for requests on page 150

Gathering further information about a request

Approvers are able to gather additional information about a request. This ability does not, however, replace granting or denying approval for a request. There is no additional approval step required in the approval workflow to obtain the information.

Approvers can request information in form of a question from anybody. The request is placed on hold for the period of the inquiry. Once the queried identity has supplied the necessary information and the approver has made an approval decision, the request is taken off hold. The approver can recall a pending inquiry at any time. The request is taken off hold. The approver's request and the identity's answer are recorded in the approval flow and are therefore available to the approver.

NOTE: If the approver who made the query is dropped, hold status is revoked. The queried identity must not answer. The request procedure continues.

For more information, see the *One Identity Manager Web Portal User Guide*.

Detailed information about this topic

- Email notification: Notifications with questions on page 188

Appointing other approvers

Once an approval level in the approval workflow has been reached, approvers at this level can appoint another identity to handle the approval. To do this, you have the options described below:

- Rerouting approvals

  The approver appoints another approval level to carry out approvals. To do this, set up a connection to the approval level in the approval workflow to which an approval decision can be rerouted.

- Appointing additional approvers

  The approver appoints another identity to carry out the approval.The other approver must make an approval decision in addition to the known approvers. To do this, enable the **Additional approver possible** option in the approval step.

  The additional approver can reject the approval and return the requests to the original approver. The original approver is informed about this by email. The original approver can appoint another additional approver.

- Delegate approval

  The approver appoints another identity to carry out the approval. This identity is added to the current approval step as the approver and then makes the approval

decision instead of the approver who delegated. To do this, enable the **Approval can be delegated** option in the approval step.

The current approver can reject the approval and return the requests to the original approver. The original approver can withdraw the delegation and delegate a different identity, for example, if the other approver is not available.

Email notifications can be sent to the original approvers and the others.

For more information, see the *One Identity Manager Web Portal User Guide*.

Detailed information about this topic

- Connecting approval levels on page 101
- Editing approval levels on page 94
- Properties of an approval step on page 95

Related topics

- Notifications in the request process on page 181
- Email notification: Delegating approvals on page 188
- Email notification: Rejecting approvals on page 188
- Email notification: Using additional approvers to approve requests on page 189
- Email notification: Scheduled request for approval on page 184

Escalating an approval step

Approval steps can be escalated under the following conditions:

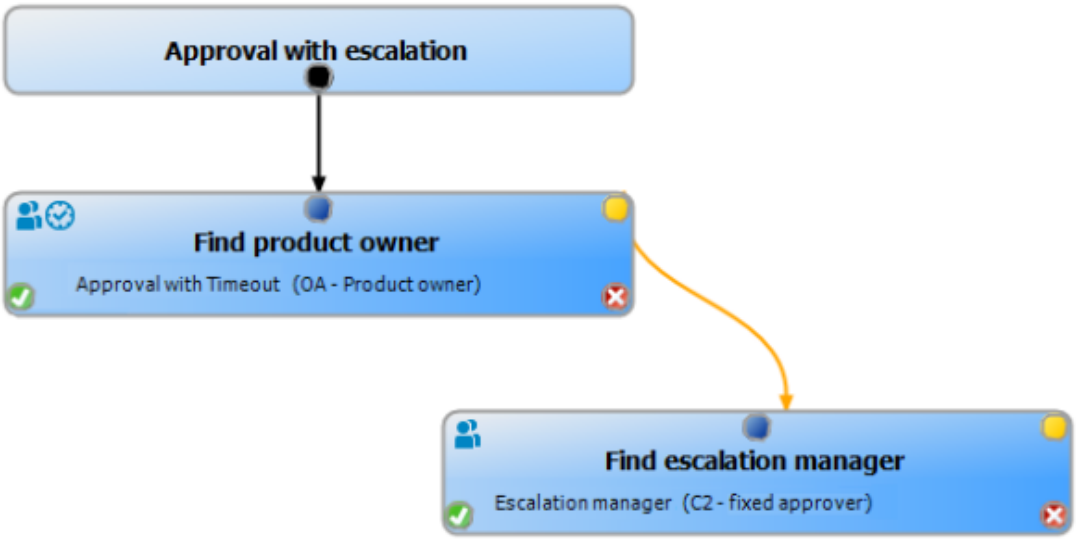
- Automatic escalation when a given time limit is exceeded.
- Manual escalation by the approver in the Web Portal

This presents the request to another approval body. The request is then further processed in the normal approval workflow.

To configure escalation of an approval step

1. Open the approval workflow in the Workflow Editor.
2. Add an additional approval level with one approval step for escalation.
3. Connect the approval step that is going to be escalated when the time period is exceeded with the new approval step. Use the connection point for escalation to do this.

Figure 8: Example of an approval workflow with escalation



4. Configure the behavior for the approval step to be escalated when it times out.

Table 41: Properties for escalation on timeout

Property	Meaning
Timeout (minutes)	Time interval after which the approval step automatically handles the approval decision. The input is converted into working hours and displayed additionally. • From the drop-down, select the unit of time and enter an appropriate value. The working hours of the respective approver are taken into account when the time is calculated. NOTE: Ensure that a state, county, or both is entered into the identity's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating identities' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*. TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.

Property	Meaning
	If more than one approver was found, then an approval decision for the approval step is not automatically made until the timeout for all approvers has been exceeded. The same applies if an additional approver has been assigned. If an approver delegated approval, the time point for automatic approval is recalculated for the new approver. If this approval is rejected, the time point for automatic approval is recalculated for the original approver. If an approver is queried, the approval decision must be made within the defined timeout anyway. The time point for automatic approval is not recalculated. If additional approvers are determined by recalculating the current approvers, then the automatic approval deadline is not extended. The additional approvers must approve within the time frame that applies to the current approver.
Timeout behavior	Action that is run if the timeout expires. • **`Escalation`**: The request process is escalated. The escalation approval level is called.

5. (Optional) If the approval step still needs to be escalated but no approver be found and no fallback approver is assigned, set the **Escalate if no approver found** option.

   In this case, the request is escalated instead of being canceled or passed to the chief approval team.

In the event of an escalation, email notifications can be sent to the new approvers and requesters.

Related topics

- Email notification: Requesting approval on page 182
- Email notification: Escalating requests on page 187

Approvers cannot be established

You can specify a fallback approver if requests cannot be approved because no approvers are available. A request is then always assigned to the fallback approver for approval no approver can be found in an approval step in the specified approval procedure.

To specify fallback approvers, define application roles and assign these to an approval step. Different approval groups in the approval steps may also require different fallback approvers. Specify different application role for this, to which you can assign identities who

can be determined as fallback approvers in the approval process. For more information, see the *One Identity Manager Authorization and Authentication Guide*.

To specify fallback approvers for an approval step

- Enter the following data for the approval step.

Table 42: Approval step properties for fallback approvers

Property	Meaning
Fallback approver	Application role whose members are authorized to approve requests if an approver cannot be determined through the approval procedure. Assign an application from the drop-down. To create a new application role, click . Enter the application role name and assign a parent application role. For more information, see the *One Identity Manager Authorization and Authentication Guide*. NOTE: The number of approvers is not applied to the fallback approvers. The approval step is considered approved the moment as soon as one fallback approver has approved the request.

Request sequence with fallback approvers

1. No approver can be found for an approval step in an approval process. The request is assigned to all members of the fallback approver application role.
2. Once a fallback approver has approved a request, it is presented to the approvers at the next approval level.

   NOTE:In the approval step, you can specify how many approvers must make a decision on this approval step. This limit is NOT valid for the chief approval team. The approval step is considered to be approved as soon as ONE fallback approver has approved the request.
3. The request is canceled if no fallback approver can be found.

Fallback approvers can make approval decisions on requests for all manual approval steps. Fallback approvals are not permitted for approval steps using the CR, SB, CD, EX, and WC approval procedures or OC and OH approval procedures.

Related topics

- Editing approval levels on page 94
- Selecting responsible approvers on page 105
- Approval by the chief approval team on page 161
- Escalating an approval step on page 155

Automatic approval on timeout

Requests can be automatically granted or denied approval once a specified time period has expired.

To configure automatic approval if the timeout expires

- Enter the following data for the approval step.
  - **Timeout (minutes)**:

    Time interval after which the approval step automatically handles the approval decision. The input is converted into working hours and displayed additionally.

    - From the drop-down, select the unit of time and enter an appropriate value.

    The working hours of the respective approver are taken into account when the time is calculated.

    NOTE: Ensure that a state, county, or both is entered into the identity's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating identities' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*.

    TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.

    If more than one approver was found, then an approval decision for the approval step is not automatically made until the timeout for all approvers has been exceeded. The same applies if an additional approver has been assigned.

    If an approver delegated approval, the time point for automatic approval is recalculated for the new approver. If this approval is rejected, the time point for automatic approval is recalculated for the original approver.

    If an approver is queried, the approval decision must be made within the defined timeout anyway. The time point for automatic approval is not recalculated.

    If additional approvers are determined by recalculating the current approvers, then the automatic approval deadline is not extended. The additional approvers must approve within the time frame that applies to the current approver.
  - **Timeout behavior**:

    Action, which is run if the timeout expires.

- **Approved**: The request is approved in this approval step. The next approval level is called.
- **Deny**: The request is denied in this approval step. The approval level for denying is called.

If a request is decided automatically, the requester can be notified by email.

Related topics

- Email notification: Approving or denying request approval on page 185
- Editing approval levels on page 94

Halting a request on timeout

Requests can be automatically halted once a specified time period has been exceeded. The action halts when either a single approval step or the entire approval process has exceeded the timeout.

To configure halting after the timeout of a single approval step has been exceeded

- Enter the following data for the approval step.
  - **Timeout (minutes)**:

    Time interval after which the approval step automatically handles the approval decision. The input is converted into working hours and displayed additionally.

    - From the drop-down, select the unit of time and enter an appropriate value.

    The working hours of the respective approver are taken into account when the time is calculated.

    NOTE: Ensure that a state, county, or both is entered into the identity's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating identities' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*.

    TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.

    If more than one approver was found, then an approval decision for the approval step is not automatically made until the timeout for all approvers has been exceeded. The same applies if an additional approver has been assigned.

If an approver delegated approval, the time point for automatic approval is recalculated for the new approver. If this approval is rejected, the time point for automatic approval is recalculated for the original approver.

If an approver is queried, the approval decision must be made within the defined timeout anyway. The time point for automatic approval is not recalculated.

If additional approvers are determined by recalculating the current approvers, then the automatic approval deadline is not extended. The additional approvers must approve within the time frame that applies to the current approver.

- **Timeout behavior**:

  Action that runs if the timeout expires.

  - `Cancel`: The approval step, and therefore the entire approval process for the request, is canceled.

To configure halting on timeout for the entire approval process

- Enter the following data for the approval workflow.
  - **System halt (days)**:

    Number of days to elapse after which the approval workflow, and therefore the system, automatically halts the entire approval process.

If a request is halted, the requester can be notified by email.

Related topics

- Email notification: Canceling requests on page 187
- Editing approval levels on page 94
- Setting up approval workflows on page 93

Approval by the chief approval team

Sometimes, approval decisions cannot be made for requests because the approver is not available or does not have access to One Identity Manager tools. To complete these requests, you can define a chief approval team whose members are authorized to intervene in the approval process at any time.

The chief approval team is authorized to approve, deny, or cancel requests in special cases or to authorize other approvers.

IMPORTANT:

- The four-eye principle can be broken like this because chief approval team members can make approval decisions for requests at any time. Specify, on a custom basis, in which special cases the chief approval team may intervene in the

approval process.

- The chief approval team members may always approval their own requests. The settings for the **QER | ITShop | PersonInsertedNoDecide** and **QER | ITShop | PersonOrderedNoDecide** configuration parameters do not apply for the chief approval team.
- Approvals made by the chief approval team are not automatically transferred to other approval levels. Settings for the **QER | ITShop | DecisionOnInsert**, **QER | ITShop | AutoDecision** and **QER | ITShop | ReuseDecision** configuration parameters do not apply to the chief approval team.
- In the approval step, you can specify how many approvers must make a decision on this approval step.
    - If an approval decision is made by the chief approval team, it overrides the approval decision of just one regular approver. This means, if three approvers must approve an approval step and the chief approval team makes a decision, two more are still required.
    - The number of approvers is not taken into account if the request is assigned to fallback approvers. The chief approval team can also approve in this case. The approval decision is considered to be made as soon as one member of the chief approval team has made an approval decision about the request.
- If a regular approver has added an additional approver, the chief approval team can approve for both the regular and the additional approvers. If both approvals are pending, a chief approver first replaces the regular approver's approval only. Only a second approval of the chief approval team can replace the approval of the additional approver.

The chief approval team can approve requests for all manual approval steps. The following applies:

- Chief approval team decisions are not permitted for approval steps using the CR, SB, CD, EX, and WC approval procedures or the OC and OH procedures.
- If a member of the chief approval team is identified as a regular approver for an approval step, they can only make an approval decision for this step as a regular approver.
- The chief approval team can also make an approval decision if a regular approver has submitted a query and the request is in hold status.

To add members to the chief approval team

1. In the Manager, select the **IT Shop > Basic configuration data > Chief approval team** category.
2. Select the **Assign identities** task.

   In the **Add assignments** pane, assign the identities who are authorized to approve all requests.

   TIP: In the **Remove assignments** pane, you can remove assigned identities.

To remove an assignment

- Select the identity and double-click ✓.

3. Save the changes.

Related topics

- Chief approval team on page 215
- Escalating an approval step on page 155

Approving requests with terms of use

Terms of use that explain conditions of use for a product can be stored for individual service items (for example, software license conditions). When someone requests this product, the requester, and request recipient must accept the terms of use before the request can be finalized.

In order for the request recipient to accept the terms of use, the request must be assigned to the request recipient in the approval process. Set an approval workflow for such requests that contain a BR approval step and enable the **No automatic approval** option for this approval step. One Identity Manager provides a default approval workflow and a **Terms of Use acknowledgment for third-party orders (sample)** default approval policy that you can use for this. Using the default approval workflow as a basis, create your own approval workflow that returns the request to the request recipient and determines the approver after the terms of use have been accepted. Use the BR approval procedure to do this.

To create an approval workflow for requests with terms of use

1. In the Manager, select the **IT Shop > Basic configuration data > Approval workflows > Predefined** category.
2. In the result list, select the `Terms of Use acknowledgment for third-party orders (sample)` approval workflow and run the **Change main data** task.
3. Select the **Copy workflow** task.
4. Enter a name for the copy and click **OK**.
5. Edit the copy. Modify the approval workflow to suit your requirements.
6. Create an approval policy and assign it to the approval workflow.
7. Assign service items to the approval policy, which are assigned terms of use.

Detailed information about this topic

- Setting up approval workflows on page 93
- Approval policies for requests on page 85

- General main data for service items on page 23
- Adding to the IT Shop on page 88

Using default approval processes

By default, One Identity Manager supplies approval policies and approval workflows. These are used in the approval processes of the **Identity & Access Lifecycle** shop.

Table 43: Default approval policies and workflows in the shop identity & access lifecycle

Approval policies/ workflow	Description	Shelf | Product
Compliance checking simplified	Compliance checking and exception approval for all products on the shelf that do not have their own approval policy assigned to them. For more information, see Testing requests for rule compliance on page 133.	Identity Lifecycle
Self-service	Assignment requests and delegations are automatically approved by default. For more information, see Standard products for assignment requests on page 60.	Identity Lifecycle | Delegation
		Identity Lifecycle | Business role entitlement assignment
		Identity Lifecycle | Business role membership
Self-service	Automatic approval for all products on the shelf that do not have their own approval policy assigned to them. Weitere Informationen finden Sie unter Selbstbedienung.	Group Lifecycle
		Microsoft Entra ID groups
		Microsoft Entra ID subscriptions
		Disabled Microsoft Entra ID service plans
		Exchange Online distribution groups
		Microsoft 365 groups

Approval policies/ workflow	Description	Shelf | Product
		Microsoft Teams teams
Terms of Use acknowledgment for third-party orders (sample)	Copy template for requests with terms of use. For more information, see Approving requests with terms of use on page 163.	
Challenge loss of role membership	Limited period assignment requests for role memberships are automatically granted approval. For more information, see Requests with limited validity period for changed role memberships on page 203.	Identity Lifecycle | Challenge loss of role membership
New manager assignment	Requesting a change of manager must be approved by the new manager. For more information, see Requesting change of manager for an employee on page 178.	Identity Lifecycle | New manager assignment
Approval of Active Directory group create requests	New Active Directory group requests must be approved by the target system manager. The groups are added in One Identity Manager and published in the target system. For more information about this, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.	Group Lifecycle | New Active Directory security group
		Group Lifecycle | New Active Directory distribution group
Approval of Active Directory group change requests	Changes to group type and range of Active Directory groups must be approved by the target system manager. For more information about this, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.	Group Lifecycle | Modify Active Directory group
Approval of Active Directory group deletion requests	Deleting an Active Directory group, must be approved by the target system manager. For more information about this, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.	Group Lifecycle | Delete Active Directory group
Approval of Active Directory group membership requests	Product owners and target system managers can request members for groups in these shelves. For more information about this, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.	Active Directory groups

Approval policies/ workflow	Description	Shelf | Product
Approval of SharePoint group create requests	New SharePoint group requests must be approved by the target system manager. The groups are added in One Identity Manager and published in the target system. For more information about this, see the *One Identity Manager Administration Guide for Connecting to SharePoint*.	Group Lifecycle | New SharePoint group
Approval of group membership requests	Product owners and target system managers can request members for groups in these shelves. For more information about this, see the *One Identity Manager Administration Guide for Connecting to SharePoint*.	SharePoint groups
Approval of system entitlement removal requests	This approval policy can be used to configure automatic deletion of memberships in Active Directory groups.	Approval of system entitlement removal requests
Approval of privileged access requests	Requests for access must be approved by the owner of the privileged object. To make an access request, additional system prerequisites must be met by the Privileged Account Management system. For more information about PAM access requests, see the *One Identity Manager Administration Guide for Privileged Account Governance*.	Privileged access | API key request Privileged access | File request Privileged access | Password request Privileged access | Remote desktop session request Privileged access | Remote desktop session request Privileged access | SSH key request Privileged access | SSH session request Privileged access | Telnet session request

3

Request sequence

Shop customers can request, renew, and unsubscribe products as soon as an IT Shop solution is set up. Use the Web Portal to do this. Furthermore, requests, and cancellations are approved in the Web Portal. You can make an overview of pending and closed requests for yourself. You can also find an overview of pending and closed requests in the Manager The status of pending requests is checked regularly by the DBQueue Processor. The review is started by the **IT Shop check** schedule.

Requests can have a limited time period, which means the requested product assignment is only valid within the validity period.

General request sequence

1. A customer places a request in the Web Portal for:
    a. A product.

       - OR -

    b. Membership of a hierarchical role.

       - OR -

    c. The assignment of a company resource to a hierarchical role.
2. The request goes through the assigned approval process.
3. If the request has been granted approval and the **Valid from** date has been reached:
    a. The product is assigned to the customer. The company resource associated with the product is assigned indirectly to the customer.

       - OR -

    b. The customer becomes a secondary member of the hierarchical role.

       - OR -

    c. The company resource is assigned to the hierarchical role.

    The request contains the **Assigned** status (`PersonWantsOrg.OrderState = 'Assigned'`).

    The product/membership/assignment remains until it is canceled.

Requests and the resulting assignments are displayed in the following table:

Requests	`PersonWantsOrg`
Product assignments	`PersonInITShopOrg`

Company resource assignments	For example,
	`PersonHasQERResource`
	`ADSAccountInADSGroup`

Hierarchical role assignments	For example, `PersonInDepartment`
Hierarchical role assignments	For example, `DepartmentHasADSGroup`

General cancellation sequence

1. A customer cancels a product/membership/assignment in the Web Portal.

   - OR -

   A requested product/requested membership/requested assignment is automatically unsubscribed.
2. The cancellation goes through the assigned approval process.
3. If cancellation was granted approval and the expiry date has been reached:
   a. The product's assignment is removed. The product's assigned to the associated company resource is also removed.

      - OR -

   b. The customer’s membership of the hierarchical role is removed.

      - OR -

   c. The company resource's assignment to the hierarchical role is removed.

   The request contains the **`Unsubscribed`** status (`PersonWantsOrg.OrderSTate = 'Unsubscribed'`).

If a customer is removed from a shop, existing requests for this are closed. The products are unsubscribed and assignments are removed. If the customer changes to another shop, the product requests can be retained under certain circumstances. If the request is an assignment request, it can also be retained under certain circumstances, even if the requester is no longer a customer in the shop.

For more information about requesting products, see the *One Identity Manager Web Portal User Guide*.

Related topics

- Examples of request results on page 275
- Requests with limited validity period on page 172
- Relocating a customer or product to another shop on page 176
- Removing customers from a shop on page 66
- Determining the responsible approvers on page 130

The request overview

To obtain an overview of all pending and closed requests

1. In the Manager, select the **IT Shop | Requests | <filter>** category.
2. Select a request procedure in the result list.
3. Select the **Request overview** task.

Displaying request details

To obtain detailed information about a request

1. In the Manager, select the **IT Shop | Requests | <filter>** category.
2. Select a request procedure in the result list.
3. Select the **Request details** task.

This shows you the request data and the status of the request.

Displaying the approval sequence

For pending requests, see the current status of the approval process. The approval sequence is shown as soon as the DBQueue Processor has determined the approvers for the first approval step. In the approval workflow, you can view the approval sequence, the results of each approval step, and the approvers found. If the approval procedure could not find an approver, the request is canceled by the system.

To display the approval sequence of a pending request

1. In the Manager, select the **IT Shop > Requests > Pending requests > <filter>** category.
2. Select a request procedure in the result list.
3. Select the **Approval sequence** task.

Each approval level of an approval workflow is represented by a special control. The approvers responsible for a particular approval step are shown in a tooltip. Pending attestation questions are also shown in tooltips. These elements are shown in color, the color code reflecting the current status of the approval level.

Table 44: Meaning of the colors in an approval sequence (in order of decreasing importance)

Color	Meaning
Blue	This approval level is currently being processed.
Green	This approval level has been granted approval.
Red	This approval level has been denied approval.
Yellow	This approval level has been deferred due to a question.
Gray	This approval level has not (yet) been reached.

Displaying the approval history

The approval history displays each step of the request process. Here you can follow all the approvals in the approval process in a chronological sequence. The approval history is displayed for both pending and closed requests.

To view the approval history for a request

1. In the Manager, select the **IT Shop | Requests | <filter>** category.
2. Select a request procedure in the result list.
3. Select the **Approval history** task.

These elements are shown in color, the color code reflecting the status of the approval steps.

Table 45: Meaning of colors in the approval history

Color	Meaning
Yellow	Request triggered.
Green	Approver has granted approval.
Red	Approver has denied approval. Request has been escalated. Approver has recalled the approval decision.
Gray	Product has been canceled. Request has been canceled. Request has been assigned to an additional approver. Additional attestor has withdrawn approval decision. Approval has been delegated New attestor has withdrawn the delegation.

Color	Meaning
	Request has been transferred to another shop. Request recipient has been changed. Request has been converted into a direct assignment.
Purple	Request renewed.
Orange	Approver has a query. The query has been answered. Query was canceled due to change of approver.
Blue	Approver has rerouted approval. The approval step was reset automatically.

Requesting products more than once

The IT Shop distinguishes between single or multiple requestable products. Single request products are, for example, software, system roles, or Active Directory groups. These products cannot be requested if they have already been be requested for the same time period.

Furthermore, there may be company resources that are needed more than once, consumables, for example. You can find company resources such as these mapped in One Identity Manager as **Multi-request resource** or **Multi requestable/unsubscribable resources**.

Request sequence of multi-request resources

1. A customer requests a multi-request resource in the Web Portal.
2. The request goes through the appropriate approval process and is approved.

   The request is only saved in the `PersonWantsOrg` table. No entry is created in the `PersonInITShopOrg` table.
3. The resource can be canceled immediately. The request contains the **`Unsubscribed`** status (`PersonWantsOrg.OrderState = 'Unsubscribed'`).

   The resource cannot be canceled by the customer.

Request sequence of multi requestable/unsubscribable resources

1. A customer requests a multi requestable/unsubscribable resource in the Web Portal.
2. The request goes through the appropriate approval process and is approved.

   The request is only saved in the `PersonWantsOrg` table. No entry is created in the `PersonInITShopOrg` table.

3. The request contains the **Assigned** status (`PersonWantsOrg.OrderState = 'Assigned'`).

   The resource can be unsubscribed by means of the Web Portal.

TIP: A customer-specific implementation of a process with the `PersonWantsOrg` root object for the `OrderGranted` result can be made in order to start a specified action when a multi-request resource is approved. For more information about defining processes, see *One Identity Manager Configuration Guide*.

Related topics

- Multi-request resources on page 19
- Examples of request results on page 275

Requests with limited validity period

Customers keep their requested products on the shelf until they themselves unsubscribe from them. 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 labeled with the validity period. For more information, see Products for requests with time restrictions on page 48.

When a product with a limited request period is requested, One Identity Manager calculates the date and time at which the product is automatically unsubscribed (**Valid until**/expiry date of the request) from the current date and validity period specified in the service item. This deadline can be adjusted when the request is made.

As soon as a request is approved by all approvers, the expiration date is recalculated from the actual date and the validity period. This ensures that the validity period is valid from the day of assignment.

A **Valid from** date can also be entered at the time of request. This specifies the date that an assignment starts to apply. If this date is given, the expiry date is calculated from the **Valid from** date and the validity period. If both a validity period and a **Valid from** date are specified and the **Valid from** date is in the future, then the expiration date is not recalculated. The request remains valid until the specified **Valid until** date. If the validity period has already expired at the time of approval, the request can no longer be approved. The request is canceled and an error message is displayed.

Cancellations can include a validity period, which means a deadline for the cancellation is set for unlimited requests. Use this method to change the expiry date for requests with a validity period. Once the cancellation has been granted approval, the cancellation's validity period is taken as the new expiry date of the request. The request cannot be extended beyond the validity period.

Multiple requests for a product with limited validity period

If a customer has requested a product with a limited validity period, the validity period must be tested for validity in subsequent requests for this product for the same customer.

If the validity period is not in effect, the request is not permitted. By default, new requests are permitted if they fall in a time period that is not covered by another pending request. However, the validity periods of different requests may not overlap. You can define the desired behavior for the validity period over configuration parameters. For more information, see Checking request validity periods on page 174.

Related topics

- Renewing requests on page 173
- Canceling or unsubscribing requests on page 174

Renewing requests

The request recipient receives a message before reaching the expiry date and has the possibility to extend the period. For more information, see Sequence for limited requests on page 184. The request is canceled once the expiry date has been reached.

The customer has the option to renew a request. If the customer uses this option, the extension (as in the original request) needs to approved through an approval process. The renewal workflow stored with the approval policy is used for this purpose. If the extension is denied, the original request runs out at the given date. You can also limit renewals in the same way. The renewal's expiration date is calculated from the date of the renewal's approval and the validity period of the product if no **Valid until** date was specified at the time of the renewal.

A limited request might look like the following a sequence:

Service item	Validity period: 90 days
Requested on: 1/2/2017	Valid until: 4/1/2017 11:59 PM
Approved on: 1/5/2017	Valid until: 4/5/2017 11:59 PM
Renewed until: 3/31/2017	Renewal valid until: 4/30/2017 12:00 PM
Approved on: 4/2/2017	Valid until: 4/30/2017 12:00 PM
Canceled on: 4/10/2017	Unsubscribed as from: 4/14/2017 11:59 PM
Approved on: 4/11/2017	Valid until: 4/11/2017 11:59 PM

NOTE: Ensure that times in the One Identity Manager tools, for example, the Web Portal, are in the user's local time.

Related topics

- Requests with limited validity period on page 172
- Canceling or unsubscribing requests on page 174

Canceling or unsubscribing requests

DBQueue Processor checks whether the request's expiry date has passed using a scheduled One Identity Manager task, which compares it against current UTC time. If the expiry date has passed, the request is canceled; the resulting assignments removed. You can configure this behavior.

If necessary, temporary requests can be unsubscribed. If the expiry date has passed, the unsubscription workflow stored at the decision guideline is run in this case. The unsubscription must be approved; only then will the assignment be permanently removed. If another request exists for the product, perhaps with the status **Pending**, the expired request will be canceled and replaced by the pending request.

To unsubscribe temporary requests on expiry

- In the Designer, set the **QER | ITShop | ExceededValidUntilUnsubscribe** configuration parameter.

If the configuration parameter is set, requests with the status **Assigned** or **Renewal** will be unsubscribed. The unsubscription workflow entered in the approval policy runs through if no other request exists for the product, which now takes effect. Once the unsubscription is approved, the assignment will be removed. Expired requests with the status **approved, pending, request** are canceled.

NOTE: If the unsubscription is denied, the approver must enter a new **Valid until** date. Otherwise, the request is given **Assigned** status and the unsubscription workflow runs again.

Related topics

- Requests with limited validity period on page 172
- Renewing requests on page 173

Checking request validity periods

If a customer has requested a product with a limited validity period, the validity period must be tested for validity in subsequent requests for this product for the same customer. If the validity period is not in effect, the request is not permitted. By default, new requests are permitted if they fall in a time period that is not covered by another pending request. However, the validity periods of different requests may not overlap. You can define the desired behavior for the validity period over configuration parameters. The configuration parameters are set by default. In this check, all requests of the same product for the same request recipient are taken into account even if the product came from different shelves.

To define differing behavior

- In the Designer, enable the desired option for the **QER | ITShop | GapBehavior | GapDefinition** and **QER | ITShop | GapBehavior | GapFitting** configuration parameters.

Table 46: Effect of the QER | ITShop | GapBehavior | GapDefinition configuration parameter

Option	Description
0	Only pending requests are taken into account by the check. (default)
1	Only approved requests are taken into account by the check.
2	Only assigned requests are taken into account by the check.

Table 47: Effect of the QER | ITShop | GapBehavior | GapFitting configuration parameter

Option	Description
0	Validity periods can overlap. (default) A new request is accepted if its validity period fits into at least one free time slot between two existing requests.
1	Validity periods cannot overlap. A new request is accepted if its validity period fits exactly into a free time slot between two existing requests.
2	The validity period is not checked. A request is accepted even if there is already a request for the same validity period.

If the configuration parameters are disabled, One Identity Manager behaves as in option **0**.

Figure 9: Example of possible validity period for GapDefinition = 0 and GapFitting = 0

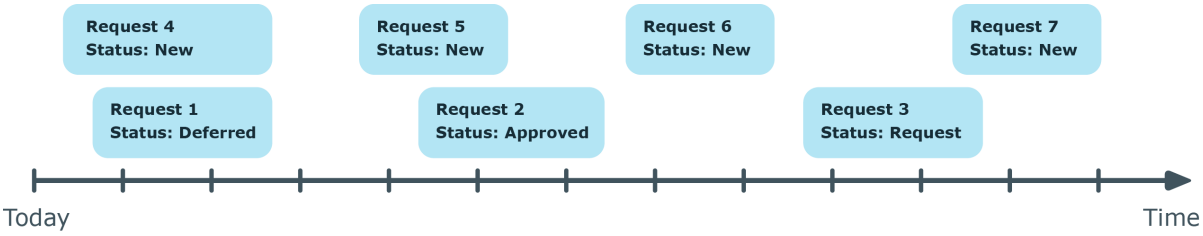
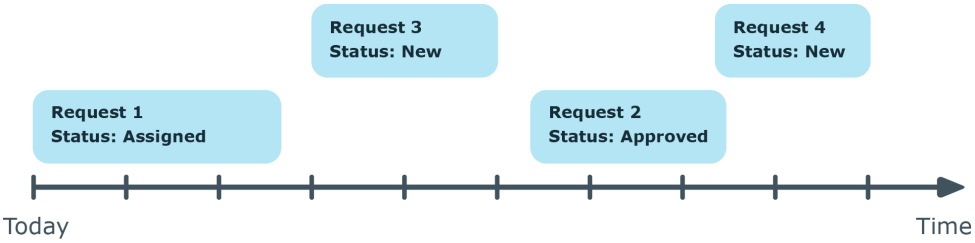


Figure 10: Example of possible validity period for GapDefinition = 1 and GapFitting = 1



Related topics

- Request statuses on page 273

Relocating a customer or product to another shop

If a customer requests a product from a shop or shopping center and then changes to another at a later date, the product request is closed and the product is canceled. The same applies if a requested product is moved to another shelf.

You can label product service items with **Retain service item assignment on relocation** to retain their requests when they relocate. All pending or approved requests in the shop are transferred to any shop in which the identity is a customer and that contains the requested products. In connection with this, pending requests are reset, which means the requests have to go through the approval process from the beginning again.

Detailed information about this topic

- Product request on customer or product relocation on page 49

Related topics

- Removing customers from a shop on page 66

Changing approval workflows of pending requests

When approval workflows are changed, a decision must be made as to whether these changes should be applied to pending requests. Configuration parameters are used to define the desired procedure.

Scenario: Another approval workflow was stored with the approval policy

If changes have been made to the approval, renewal, or cancellation workflow in an approval policy, any pending approval processes are continued by default with the original workflow. The newly stored workflow is only used in new requests. You can configure different behavior.

To specify how to handle pending requests

- In the Designer, enable the **QER | ITShop | OnWorkflowAssign** configuration parameter and select one of the following values.
    - **CONTINUE**: Ongoing approval processes are continued with the originally applicable workflow. The newly stored workflow is only used in new requests.

      This behavior also applies if the configuration parameter is not set.
    - **RESET**: In ongoing approval processes, all approval decisions already taken are reset. The approval processes are restarted with the newly stored workflow.
    - **ABORT**: Ongoing approval processes are stopped. All pending requests are closed. The customer must request, renew, or cancel the product again, if required.

A working copy of the originally applicable workflow is saved. The working copy is retained as long as it is used in ongoing approval processes. All unused working copies are regularly deleted using the **Maintenance approval workflows** schedule.

If the assigned renewal or cancellation workflow is deleted, any ongoing approval processes are stopped.

Scenario: A change was made to an approval workflow in use

If changes have been made to an approval workflow that is being used in pending requests, any pending approval processes are continued by default with the original workflow. The changes to the approval workflow are only implemented for new requests. You can configure different behavior.

To specify how to handle pending requests

- In the Designer, enable the **QER | ITShop | OnWorkflowUpdate** configuration parameter and select one of the following values.
    - **CONTINUE**: Ongoing approval processes are continued with the originally applicable approval workflow. The changes to the approval workflow are only implemented for new requests.

      This behavior also applies if the configuration parameter is not set.
    - **RESET**: In ongoing approval processes, all approval decisions already taken are reset. The approval processes are restarted with the changed approval workflow.

- **ABORT**: Ongoing approval processes are stopped. All pending requests are closed. The customer must request, renew, or cancel the product again, if required.

A working copy of the approval workflow that contains the original version is saved. This working copy is retained as long as it is used in ongoing approval processes. All unused working copies are regularly deleted using the **Maintenance approval workflows** schedule.

Related topics

- Determining the responsible approvers on page 130

Requests for employees

In the Web Portal default installation, approvers can request and cancel products for other users. Approvers can only request products for users of shops they manage and where the user is an customer. Furthermore, department managers and their deputies may edit the data for employees belonging to their department.

The responsibilities are evaluated through the following database view (View).

QER_VEditEmployee	This view displays the department manager, their deputies, and employees whose data can be edited.

Requesting change of manager for an employee

Managers can edit main data of their employees in the Web Portal. In the same context, it is possible to define a new manager for an employee. To do this, the previous manager requests assignment of another manager. If the other manager agrees to the assignment, they are assigned to the employee as manager.

Prerequisites

The following objects are made available in the One Identity Manager database by default:

Table 48: Default objects for the change of manager

Objects	Description
New manager assignment multi-request	Is used to request the other manager in the IT Shop. The product is canceled the moment the new manager has been

Objects	Description
resource	assigned. The **New manager assignment** service item is assigned.
New manager assignment service item	Product that is ordered when another manager is assigned. The **New manager assignment** approval policy is assigned.
Identity & Access Lifecycle | Identity Lifecycle IT Shop structure	The service item is assigned by default to the **Identity Lifecycle** shelf in the **Identity & Access Lifecycle** shop.
New manager assignment approval policy	This specifies the approval workflow by which the change of manager is approved. It is assigned to the approval workflow, **New manager assignment**.
New manager assignment approval workflow	This determines the other manager as an approver. If this is denied, the request is returned to the previous manager.
`VI_ESS_PersonWantsOrg_Set_New_Person.Manager` process	Allocates the other manager to the identity as manager as soon as the change of manager was approved and the validity period of the request is reached.

Procedure for changing managers

1. The previous manager edits the main data of the employee the other manager is going to take on. They select an identity as manager and specify a date from which the changes take effect.

   Table 49: Changes that are requested

Property	Description
New manager	Identity to be assigned as a new manager for the employee.
Effective date	The date on which the change takes effect.
Changes to be run after approval is granted	Changes that should be run after approval has been granted and the new manager has been assigned, for example, deleting user accounts or removing memberships in system entitlements. The previous manager can decide which of the changes listed should be run.

2. A request with the following properties is triggered.

Table 50: Properties of the manager change request

Property	Description
Requester	Previous manager.
Recipient	Employee.
Additional request data	New manager.
Approver	New manager.
Valid from	The date on which the change takes effect.
Additional data	Additional changes to be run.

3. The request is assigned for approval to the new manager, who can also specify what other changes should be made after the manager has been replaced.
    a. If the manager denies approval, the request is returned to the previous manager.

       This manager can select another manager and approve the request. The request is assigned to this other manager for approval.

       The previous manager can deny request approval. The change of manager is closed. The employee's manager is not changed.

    b. If the new manager grants approval to the request, they are assigned as manager to the identity from the validity date of the request. All selected additional changes are also run on the validity date.
4. Product is unsubscribed. The request is closed.

For more information about assigning a new manager, see the *One Identity Manager Web Portal User Guide*.

Canceling requests

Request recipients, requesters, and the members of the chief approval team can cancel requests that have not already be approved in the Web Portal. The approval process is canceled immediately. The request is given the **Canceled** status.

For more information about canceling processes in the Web Portal, see the *One Identity Manager Web Portal User Guide*.

To cancel a request in the Manager

1. In the Manager, select the **IT Shop > Requests > Pending requests > <filter> > <request>** category.
2. Select a request procedure in the result list.
3. Click **Cancel request**.

4. Confirm the security prompt with **Yes**.
5. Click **OK**.

Unsubscribe products

Assigned products that are no longer needed can be unsubscribed. Each request undergoes an approval process. If an unsubscription workflow is stored with the approval policy, unsubscription is approved or denied by an approver. If there is no unsubscription workflow given, unsubscription is approved immediately.

If the request's **Valid until** date has already expired and unsubscription is likely to be denied, the approver must enter a new **Valid until** date.

Request recipients can be notified if a request is unsubscribed by another identity.

Related topics

- Request sequence on page 167
- Requests with limited validity period on page 172
- General main data of approval policies on page 86
- Unsubscribing approved requests on page 190

Notifications in the request process

In a request process, various email notifications can be sent to requesters and approvers. The notification procedure uses mail templates to create notifications. The mail text in a mail template is defined in several languages. This ensures that the language of the recipient is taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

Messages are not sent to the chief approval team by default. Fallback approvers are only notified if not enough approvers could be found for an approval step.

To use email notifications

1. Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.
2. In the Designer, set the **QER | ITShop | DefaultSenderAddress** configuration parameter and enter the sender address used to send the email notifications.
3. Ensure that all identities have a default email address. Notifications are sent to this address. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

4. Ensure that a language can be determined for all identities. Only then can they receive email notifications in their own language. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.
5. Configure the notification procedure.

Related topics

- Custom mail templates for notifications on page 243

Requesting approval

When a customer requests a product, the approver is notified that new approvals are pending.

Prerequisite

- The **QER | ITShop | MailTemplateIdents | RequestApproverByCollection** configuration parameter is not set.

To set up the notification procedure

- On the **Mail templates** tab of the approval step, enter the following data:

  Mail template request: IT Shop Request - approval required

  TIP: To allow approval by email, select the **IT Shop Request - approval required (by email)** mail template.

NOTE: You can schedule requests for approval to send a general notification if there are requests pending. This replaces single requests for approval at each approval step.

Related topics

- Email notification: Scheduled request for approval on page 184
- Approval by mail on page 191
- Editing approval steps on page 95

Reminding approvers

If an approver has not made a decision by the time the reminder timeout expires, notification can be sent by email as a reminder. The approvers working hours are taken into account when the time is calculated.

Prerequisite

- The **QER | ITShop | MailTemplateIdents | RequestApproverByCollection** configuration parameter is not set.

To set up the notification procedure

- Enter the following data for the approval step.
  - **Reminder after (minutes)**:

    Time interval after which the approver is notified by mail that there are still pending requests for approval. The input is converted into working hours and displayed additionally.

    - From the drop-down, select the unit of time and enter an appropriate value.

    NOTE: Ensure that a state, county, or both is entered into the identity's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating identities' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*.

    TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.

    If more than one approver was found, each approver will be notified. The same applies if an additional approver has been assigned.

    If an approver delegated the approval, the time point for reminding the delegation recipient is recalculated. The delegation recipient and all the other approvers are notified. The original approver is not notified.

    If an approver has made an inquiry, the time point for reminding the queried identity is recalculated. As long as the inquiry has not been answered, only this identity is notified.
  - **Mail template reminder**: Select the **IT Shop request - remind approver** mail template.

    TIP: To allow approval by email, select the **IT Shop Request - remind approver (by email)** mail template.

NOTE: You can schedule requests for approval to send a general notification if there are requests pending. This replaces single requests for approval at each approval step.

Related topics

- Email notification: Notifications with questions on page 188
- Email notification: Scheduled request for approval on page 184

- Approval by mail on page 191
- Editing approval steps on page 95

Scheduled request for approval

Approvers can be regularly notified of requests that are pending. These regular notifications replace the individual prompts and approval reminders that are configured in the approval step.

To send regular notifications about pending requests

1. Enable the **QER | ITShop | MailTemplateIdents | RequestApproverByCollection** configuration parameter in the Designer.

   By default, a notification is sent with the **IT Shop request - pending requests for approver** mail template.

   TIP: To use something other than the default mail template for these notifications, change the value of the configuration parameter in the Designer.

2. In the Designer, configure and enable the **Inform approver about pending requests** schedule.

   For more information about this, see the *One Identity Manager Operational Guide*.

Sequence for limited requests

A recipient keeps a product on the shelf up to a specific point in time when they unsubscribe the products again. Sometimes, however, products are only required for a certain length of time and can be canceled automatically. The recipient is notified by email before the expiry date is reached and has the option to renew the request.

To set up the notification procedure

1. In the Designer, set the **QER | ITShop | ValidityWarning** configuration parameter and enter the warning period (in days) for expiring requests.
2. In the Designer, configure and activate the **Reminder for IT Shop requests that expire soon** schedule.
3. Enter the following data for the approval policy:
   - **Mail template expired**: Select the mail template to be used for the email notification. The default installation provides the **IT Shop request - product expires** and **IT Shop request - expired** mail templates.
4. Save the changes.

Related topics

- Requests with limited validity period on page 172
- Approval policies for requests on page 85

Approving or denying request approval

When a request is granted approval or denied, the request recipient is notified by email. Notification may occur after approval or denial of a single approval step or once the entire approval process is complete. Requests can be automatically granted or denied approval once a specified time period has expired. The recipient is notified in the same way in this case.

To set up the notification procedure

- If notification should be sent immediately after an approval decision is made for a single approval step, enter the following data on the **Mail templates** tab of the approval step.
  - **Mail template approved**: IT Shop request - approval granted for approval step
  - **Mail template denied**: IT Shop request - approval not granted for approval step
- Enter the following data in the approval policy when notification should immediately follow the approval decision of the entire approval process:
  - **Mail template approved**: IT Shop request - approval granted
  - **Mail template denied**: IT Shop request - approval not granted

Related topics

- Approval policies for requests on page 85
- Editing approval steps on page 95

Notifying delegates

If required, a delegator can receive notifications if the deputy or recipient of the single delegation has made a request in the IT Shop. Notification is sent once an identity has been determined as an approver on the basis of a delegation and has made an approval decision for the request.

To send notification when the identity who was delegated an approval approves or denies the request

- In the Designer, set the **QER | ITShop | Delegation | MailTemplateIdents | InformDelegatorAboutDecisionITShop** configuration parameter.

  By default, a notification is sent with the **Delegation - inform delegator about decided request** mail template.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Delegations are taken into account in the following default approval procedures.

Table 51: Delegation relevant default approval procedures

Delegation of	Approval procedure
Department responsibilities	D0, D1, D2, DM, DP, MS
Cost center responsibilities	P0, P1, P2, PM, PP, MS
Location responsibilities	MS
Business role responsibilities	OM, MS
Identity responsibilities	CM
IT Shop structure responsibilities	H0, H1, H2
Memberships in business roles	OR
Memberships in application roles	DI, DR, ID, IL, IO, IP, OA, OC, OH, PI, PR, RD, RL, RO, RP, TO

Example

Jan User3 is responsible for the R1 business role. They delegate their responsibility for the business role to Jo User1. Jo User1 is themselves responsible for R2 business role.

A member of the R1 business role requests a product in the IT Shop. In the approval process, Jan User3 is established as an approver through the **OM - Manager of a specific role** approval procedure. The request is assigned to Jo User1 for approval through delegation. Jan User3 is notified about the request as soon as Jo User1 has made their approval decision.

A member of the R2 business role requests a product in the IT Shop. In the approval process, Jo User1 is established as the approver through the **OM - Manager of a specific role** approval procedure. No notification is sent because Jo User1 does not make the approval decision due to delegation.

Bulk delegation

You have the option to delegate all your responsibilities to an identity in the Web Portal. If you have a lot of responsibilities, it is possible that not all the delegations are carried out. A delegator can send a notification to themselves if an error occurs.

Detailed information about this topic

- Bulk delegation notifications on page 191

Related topics

- Default approval procedures on page 105
- Using additional approvers to approve requests on page 189

Canceling requests

Requests can be automatically canceled for various reasons, for example, when a specified time period has expired or if no approver can be found. The request recipient is notified.

To set up the notification procedure

- In the approval policy, on the **Mail templates** tab, enter the following data.

  Mail template stopped: IT Shop request - canceled

Related topics

- Editing approval steps on page 95

Escalating requests

Requests can be escalated. If a request is escalated, the requester can be notified by email.

To set up the notification procedure

- On the **Mail templates** tab of the approval step, enter the following data:

  Mail template escalation: IT Shop request - Escalation

Related topics

- Editing approval steps on page 95

Delegating approvals

If, in an approval step, other approvers can be authorized to make the approval decision, the additional approvers can be prompted to approve by email. The same applies if the approval can be delegated.

To set up the notification procedure

- On the **Mail templates** tab of the approval step, enter the following data:

  Mail template delegation: IT Shop Purchase order - Delegated/additional approval

  TIP: To enable approval by email, select the **IT ShopRequest - delegated/additional approval (by email)** mail template.

Related topics

- Approval by mail on page 191
- Appointing other approvers on page 154
- Editing approval steps on page 95

Rejecting approvals

The original approver must be notified if an additional approver or identity to whom an approval has been delegated refuses the approval.

To set up the notification procedure

- On the **Mail templates** tab of the approval step, enter the following data:

  Mail template rejection: IT Shop Purchase order - Reject approval

  TIP: If you allow approval by email, select the mail template **IT Shop request - reject approval (by mail)**.

Related topics

- Approval by mail on page 191
- Editing approval steps on page 95

Notifications with questions

Identities can be notified when a question about a request is asked. Similarly, the approvers can also be notified as soon as the question is answered.

To send a notification when an approver asks a question

- In the Designer, enable the **QER | ITShop | MailTemplateIdents | QueryFromApprover** configuration parameter.

  A notification is sent by default with the **IT Shop Request - question** mail template.

To send a notification to the approver when the queried identity answers a question

- In the Designer, set the **QER | ITShop | MailTemplateIdents | AnswerToApprover** configuration parameter.

  A notification is sent by default with the **IT Shop Request - answer** mail template.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Using additional approvers to approve requests

The original approver can be notified when an additional approver or an identity who has been delegated an approval has granted or denied the request. This mail is send the moment the approval step has been decided.

To send a notification when the additional approver approves or denies the request

- In the Designer, set the **QER | ITShop | MailTemplateIdents | InformAddingPerson** configuration parameter.

  A notification is sent by default with the **IT Shop request - approval of added step** mail template.

To send notification when the identity who was delegated an approval approves or denies the request

- In the Designer, set the **QER | ITShop | MailTemplateIdents | InformDelegatingPerson** configuration parameter.

  A notification is sent by default with the **IT Shop request - approval of delegated step** mail template.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Unsubscribing approved requests

Request recipients can be notified if a request is unsubscribed by another identity. The email is sent immediately after approval has been granted for unsubscribing.

To set up the notification procedure

- Enter the following data for the approval policy:

  Mail template canceled: IT Shop request - Canceled

Related topics

- Approval policies for requests on page 85

Renewing approved requests

Request recipients can be notified when a request has been renewed. The email notification is sent immediately after approval for the renewal has been granted.

To set up the notification procedure

- Enter the following data for the approval policy:

  Mail template renewed: IT Shop request - Renewed

Related topics

- Approval policies for requests on page 85

Product change notifications

Identities can be notified when a product is replaced by another product on a fixed date. The request recipient is automatically notified by email once notification procedures are in place and the **Change product** task is run.

TIP:

To use different mail template than the default for this notification

1. Open the `VI_ESS_PersonWantsOrg Send Mail Product Expires Soon` process in the Designer.
2. Change the process properties in the pre-script for generating the `UID_RichMail`.
3. Select the **Database > Save to database** and click **Save**.

Detailed information about this topic

- Notifications in the request process on page 181

Default mail templates

One Identity Manager supplies mail templates by default. These mail templates are available in English and German. If you require the mail body in other languages, you can add mail definitions for these languages to the default mail template.

To edit a default mail template

- In the Manager, select the **IT Shop > Basic configuration data > Mail templates > Predefined** category.

Related topics

- Custom mail templates for notifications on page 243

Bulk delegation notifications

You have the option to delegate all your responsibilities to an identity in the Web Portal. If you have a lot of responsibilities, it is possible that not all the delegations are carried out. A delegator can send a notification to themselves if an error occurs.

To send a notification if bulk delegation fails

- In the Designer, set configuration parameter **QER | ITShop | MailTemplateIdents | InformRequestorAboutMassDelegationErrors**.

  By default, a notification using the **Delegation - mass delegation errors occurred** mail template is sent.

TIP: To use something other than the default mail template for these notifications, change the value of the configuration parameter in the Designer.

Related topics

- Bulk delegation errors on page 256

Approval by mail

To provide approvers who are temporarily unable to access One Identity Manager tools with the option of making approval decisions on requests, you can set up approvals by

email. In this process, approvers are notified by email when a request attestation case is pending their approval. Approvers can use the relevant links in the email to make approval decisions without having to connect to the Web Portal. This generates an email that contains the approval decision and in which approvers can state the reasons for their approval decision. This email is sent to a central mailbox. One Identity Manager checks this mailbox regularly, evaluates the incoming emails and updates the status of the request procedures correspondingly.

IMPORTANT: An approval cannot be sent by email if multi-factor authentication is configured for the requested product. Approval mails for such requests produce an error message.

Prerequisites

- If you use a Microsoft Exchange mailbox, configure the Microsoft Exchange with:
  - Microsoft Exchange Client Access Server version 2007, Service Pack 1 or higher
  - Microsoft Exchange Web Service .NET API Version 1.2.1, 32-bit
- If you use an Exchange Online mailbox, register an application in your Microsoft Entra ID tenant in the Microsoft Azure Management Portal. For example, One Identity Manager <Approval by mail>.

  For more information about how to register an application, see https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-authenticate-an-ews-application-by-using-oauth#register-your-application.
- The One Identity Manager Service user account used to log into Microsoft Exchange or Exchange Online requires full access to the mailbox given in the **QER | ITShop | MailApproval | Inbox** configuration parameter.
- The **QER | ITShop | MailTemplateIdents | RequestApproverByCollection** configuration parameter is not set.

To set up approval by email

1. In the Designer, set the **QER | ITShop | MailApproval | Inbox** configuration parameter and enter the mailbox to which the approval mails are to be sent.
2. Set up mailbox access.
   - If you use a Microsoft Exchange mailbox:
     - By default, One Identity Manager uses the One Identity Manager Service user account to log in to the Microsoft Exchange Server and access the mailbox.

       - OR -
     - You enter a separate user account for logging in to theMicrosoft Exchange Server for mailbox access.

- In the Designer, set the **QER | ITShop | MailApproval | Account** configuration parameter and enter the user account's name.
- In the Designer, set the **QER | ITShop | MailApproval | Domain** configuration parameter and enter the user account's domain.
- In the Designer, set the **QER | ITShop | MailApproval | Password** configuration parameter and enter the user account's password.

- If you use an Exchange Online mailbox:
  - In the Designer, set the **QER | ITShop | MailApproval | AppId** configuration parameter and enter the application ID that was generated when the application was registered in the Microsoft Entra ID tenant.
  - In the Designer, set the **QER | ITShop | MailApproval | Domain** configuration parameter and enter the domain for logging into Microsoft Entra ID.
  - In the Designer, set the **QER | ITShop | MailApproval | Password** configuration parameter and enter the client secret (application password) for the application.

3. In the Designer, set the **QER | ITShop | MailTemplateIdents | ITShopApproval** configuration parameter.

   The mail template used to create the approval decision mail is stored with this configuration parameter. You can use the default mail template or add a custom mail template.

   TIP: In this case, also change the `VI_MailApproval_ProcessMail` script.

4. Assign the following mail templates to the approval steps.

Table 52: Mail templates for approval by mail

Property	Mail template
Mail template request	IT Shop request - approval required (by mail)
Mail template reminder	IT Shop request - remind approver (by mail)
Mail template delegation	IT Shop request - delegated/additional approval (by mail)
Mail template rejection	IT Shop request - reject approval (by mail)

5. In the Designer, configure and enable the **Processes IT Shop mail approvals** schedule.

   Based on this schedule, One Identity Manager regularly checks the mailbox for new approval mails. The mailbox is checked every 15 minutes. You can change how frequently it checks, by altering the interval in the schedule as required.

To clean up a mail box

- In the Designer, set the **QER | ITShop | MailApproval | DeleteMode** configuration parameter and select one of the following values.
  - **HardDelete**: The processed email is immediately deleted.
  - **MoveToDeletedItems**: The processed email is moved to the **Deleted objects** mailbox folder.
  - **SoftDelete**: The processed email is moved to the Active Directory recycling bin and can be restored if necessary.

  NOTE: If you use the **MoveToDeletedItems** or **SoftDelete** cleanup method, you should empty the **Deleted objects** folder and the Active Directory recycling bin on a regular basis.

Related topics

- Editing approval emails on page 194
- Custom mail templates for notifications on page 243
- Requesting approval on page 182
- Reminding approvers on page 182
- Delegating approvals on page 188
- Rejecting approvals on page 188
- Preparing the IT Shop for multi-factor authentication on page 59
- Adaptive cards approval on page 195

Editing approval emails

The **Processes IT Shop mail approvals** schedule starts the `VI_ITShop_Process Approval Inbox` process. This process runs the `VI_MailApproval_ProcessInBox` script, which searches the mailbox for new approval decision mails and updates the request procedures in the One Identity Manager database. The contents of the approval decision mail are processed at the same time.

NOTE: The validity of the email certificate is checked with the `VID_ValidateCertificate` script. You can customize this script to suit your security requirements. Take into account that this script is also used for attestations by email.

If an self-signed root certification authority is used, the user account under which the One Identity Manager Service is running, must trust the root certificate.

TIP: The `VI_MailApproval_ProcessInBox` script finds the Exchange Web Service URL that uses AutoDiscover through the given mailbox as default. This assumes that the AutoDiscover service is running.

If this is not possible, enter the URL in the **QER | ITShop | MailApproval | ExchangeURI** configuration parameter.

Approval decision mails are processed with the `VI_MailApproval_ProcessMail` script. The script finds the relevant approval, sets the **Approved** option if approval is granted, and stores the reason for the approval decision with the request procedures. The approver is found through the sender address. Then the approval decision mail is removed from the mailbox depending on the selected cleanup method.

NOTE: If you use a custom mail template for the approval decision mail, check the script and modify it as required. Take into account that this script is also used for attestations by email.

Adaptive cards approval

To allow approvers who temporarily do not have access to the One Identity Manager tools to approve requests, you can send adaptive cards. Adaptive cards contain all the information about the product required for approving a request. These include:

- Current and next approver
- Approval history
- Rule violations by the request
- Option to select a default reason or enter a reason as free text
- Option to adjust the request's validity period
- Link to the request in the Web Portal

One Identity Starling Cloud Assistant uses a specified channel to post the adaptive cards to the approver, waits for a response, and send this to One Identity Manager. Currently Slack and Microsoft Teams can be used to post adaptive cards. In Starling Cloud Assistant, channels are configured and can be allocated to each recipient separately.

NOTE: In previous versions of One Identity Manager, the Starling 2FA app was available for approving requests. Starling Two-Factor Authentication and the Starling 2FA app are no longer supported. Instead, use the new functionality of adaptive cards with Starling Cloud Assistant to approve requests.

Prerequisites

- The Starling Cloud Assistant service is enabled and the usable channels are configured.

  For more information, see the *One Identity Starling Cloud Assistant User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

  Access to the following endpoints must be ensured to reach a Starling organization in the respective data center.

  - United States of America:

    https://sts.cloud.oneidentity.com (to receive an authentication token)

https://cloud-assistant-supervisor.cloud.oneidentity.com (to address the Starling Cloud Assistant API)

- European Union:

  https://sts.cloud.oneidentity.eu (to receive an authentication token)

  https://cloud-assistant-supervisor.cloud.oneidentity.eu (to address the Starling Cloud Assistant API)

- One Identity Manager is connected to One Identity Starling.

  To connect One Identity Manager to One Identity Starling

  1. Start the Launchpad.
  2. Select **Connection to Starling Cloud** and click **Run**.

     This starts the Starling Cloud configuration wizard.
  3. Follow the Starling Cloud configuration wizard's instruction.

  This sets the **QER | Person | Starling | ApiEndpoint** and **QER | Person | Starling | ApiKey** configuration parameters and enters the authentication credentials.

  For more information about One Identity Starling, see the *One Identity Starling User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

Detailed information about this topic

- Using adaptive cards for approvals on page 196

Using adaptive cards for approvals

Approvers must be registered as recipients in Starling Cloud Assistant to be able to make approval decisions about requests. Each recipient must be allocated to a channel that will be used to post the adaptive card. One Identity Manager provides adaptive cards for requesting approval of IT Shop requests in German and English. These can be customized if necessary.

By default, an approval decision must be made within 1 day. If this deadline is exceeded, the Web Portal must be used to approve the request. You can configure the deadline.

To use adaptive cards for approvals

1. In the Designer, set the **QER | Person | Starling | UseApprovalAnywhere** configuration parameter.
2. Ensure that a default email address is stored in One Identity Manager for each identity that will use adaptive cards. This address must correspond to the email address that the identity uses to log in to Microsoft Teams or Slack.

For detailed information about the default email address, see the *One Identity Manager Identity Management Base Module Administration Guide*.

3. Ensure that a language can be identified for each identity that will use adaptive cards. This allows approvers to obtain adaptive cards in their own language.

   For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

4. Any service items that will be requested by sending adaptive cards must not have the **Approval by multi-factor authentication** option enabled.

   Adaptive cards are only sent if there is no multi-factor authorization is use for approving the request.

5. Register all the identities, who are going to use adaptive cards for approving, as recipients in Starling Cloud Assistant and assign them to the channel to use.

6. Install the Starling Cloud Assistant app that matches the channel.

   Every registered identity must install this app.

   For more information, see the *One Identity Starling Cloud Assistant User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

7. (Optional) Change the timeout for adaptive cards.

   - In the Designer, set the **QER | Person | Starling | UseApprovalAnywhere | SecondsToExpire** configuration parameter and adjust the value. Enter a timeout in seconds.

8. (Optional) Provide a country-specific template for adaptive cards or make adjust the adaptive cards settings.

   If a language cannot be identified or there is no suitable template for the language found, en-US is used as fallback.

Detailed information about this topic

- General main data for service items on page 23
- Adding and deleting recipients and channels on page 197
- Creating, editing, and deleting adaptive cards for requests on page 198
- Creating, editing, and deleting adaptive cards templates for requests on page 200
- Deploying and evaluating adaptive cards for requests on page 202
- Disabling adaptive cards on page 202

Adding and deleting recipients and channels

Approvers can be registered in Starling Cloud Assistant as recipients through an IT Shop request and allocated to a channel. By default, the requests are approved immediately by self-service. Then the recipients are registered and the requested channel is assigned to

them. Once the approver has installed the Starling Cloud Assistant app, they can use adaptive cards to attest.

To add a recipient in Starling Cloud Assistant

- In the Web Portal, request the **New Starling Cloud Assistant recipient** product.

To allocate Microsoft Teams as a channel in Starling Cloud Assistant

1. In the Web Portal, request the **Teams channel for Starling Cloud Assistant recipient** product.
2. Install the Starling Cloud Assistant app for Microsoft Teams.

   For more information, see the *One Identity Starling Cloud Assistant User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

To allocate Slack as a channel in Starling Cloud Assistant

1. In the Web Portal, request the **Slack channel for Starling Cloud Assistant recipient** product.
2. Install the Starling Cloud Assistant app for Slack.

   For more information, see the *One Identity Starling Cloud Assistant User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

To delete a recipient in Starling Cloud Assistant

- Cancel the **New Starling Cloud Assistant recipient** product.

To remove a channel

- Cancel the respective product.

For more information about requesting and unsubscribing products, see the *One Identity Manager Web Portal User Guide*.

Related topics

- Adaptive cards approval on page 195
- Using adaptive cards for approvals on page 196

Creating, editing, and deleting adaptive cards for requests

One Identity Manager provides adaptive cards for requesting approval of IT Shop requests in German and English. These can be displayed in the Manager. You can create your own templates for adaptive cards, for example to make changes to the content or to provide adaptive cards in other languages. The recipient's language preferences are taken into

account when an adaptive card is generated. If a language cannot be identified or there is no suitable template for the language found, en-US is used as fallback.

To use your own adaptive cards for approving requests, configure the `QER_PWOHelperPWO approve anywhere` process accordingly.

To display an adaptive card

1. In the Manager, select the **IT Shop > Basic configuration data > Adaptive cards** category.
2. Select the adaptive card in the result list.
3. Select the **Change main data** task.
4. In the **Adaptive card templates** drop-down, select a template.

   This displays the adaptive card's definition in the **Template** field.

   - To display the entire JSON code, click .

To create an adaptive card.

1. In the Manager, select the **IT Shop > Basic configuration data > Adaptive cards** category.
2. Click in the result list.
3. Edit the adaptive card's main data.
4. Create a new template for adaptive cards.
5. Save the changes.
6. Create additional language-specific templates for this adaptive card as required and save the changes.

To use your customized adaptive card

1. In the Designer, edit the `QER_PWOHelperPWO approve anywhere` process.
   a. Select the **Send Adaptive Card to Starling Cloud Assistant** process step.
   b. Edit the value of the **ParameterValue2** parameter and replace the name and UID with the values of your customized adaptive card.
2. Save the changes.

To delete an adaptive card.

1. In the Manager, select the **IT Shop > Basic configuration data > Adaptive cards** category.
2. Select the adaptive card in the result list.
3. Click in the result list.

   This deletes the adaptive card and all the templates belonging to it.

Related topics

- Creating, editing, and deleting adaptive cards templates for requests on page 200
- Using adaptive cards for approvals on page 196
- Adding and deleting recipients and channels on page 197
- Deploying and evaluating adaptive cards for requests on page 202
- Disabling adaptive cards on page 202
- General main data for adaptive cards on page 201

Creating, editing, and deleting adaptive cards templates for requests

To use your own adaptive cards or to provide adaptive cards in other languages, create your own adaptive card's templates.

To create an adaptive card template

1. In the Manager, select the **IT Shop > Basic configuration data > Adaptive cards** category.
2. Select the adaptive card in the result list.
3. Edit the adaptive card's main data.
4. Next to the **Adaptive card templates** drop-down, click .
5. In the **Language** drop-down, select a language for the adaptive card.

   All active languages are shown. To use another language, in the Designer, enable the corresponding countries. For more information, see the *One Identity Manager Configuration Guide*.
6. In the **Template** field, write a definition for the adaptive card.
   - To display the entire JSON code, click .

   You can use the Adaptive Card Designer from Microsoft or the Visual Studio Code plugin to help.
7. Save the changes.
8. In the Designer, check the `QER_CloudAssistant_ApprovalAnywhere` script and modify it to suit your requirements.

To edit an adaptive card template

1. In the Manager, select the **IT Shop > Basic configuration data > Adaptive cards** category.
2. In the result list, select the adaptive card whose template you want to edit.
3. Select the **Change main data** task.

4. In the **Adaptive card templates** drop-down, select a template.
5. In the **Template** field, edit the adaptive card definition.
    - To edit the entire JSON code, click .
6. Save the changes.

To delete an adaptive card template

1. In the Manager, select the **IT Shop > Basic configuration data > Adaptive cards** category.
2. In the result list, select the adaptive card whose template you want to delete.
3. Edit the adaptive card's main data.
4. In the **Adaptive card templates** drop-down, select the template.
5. Click next to the drop-down.
6. Save the changes.

Related topics

- Creating, editing, and deleting adaptive cards for requests on page 198
- Deploying and evaluating adaptive cards for requests on page 202
- General main data for adaptive cards on page 201

General main data for adaptive cards

Enter the following main data for an adaptive card.

Table 53: Adaptive card main data

Property	Description
Adaptive card	Name of the adaptive card.
Description	Text field for additional explanation.
Disabled	Specifies whether the adaptive card is actively used.
Adaptive card templates	Name of templates to use with this adaptive card.
Language	The template is provided in this language. The recipient's language preferences are taken into account when an adaptive card is generated and a matching template is applied. If a language cannot be identified or there is no suitable template for the language found, en-US is used as fallback.
Template	JSON template of the adaptive card that contains placeholders for Adaptive Cards Templating.

Related topics

- Creating, editing, and deleting adaptive cards for requests on page 198
- Creating, editing, and deleting adaptive cards templates for requests on page 200
- Disabling adaptive cards on page 202

Deploying and evaluating adaptive cards for requests

Once an approver is determined in an approval step, the `QER_PWOHelperPWO approve anywhere` process runs. The process is generated if the following conditions are fulfilled:

- The approver is registered as the recipient in Starling Cloud Assistant.
- A default email address is stored for the approver.
- The **QER | Person | Starling | UseApprovalAnywhere** configuration parameter is set.
- An expiry date is entered in the **QER | Person | Starling | UseApprovalAnywhere | SecondsToExpire** configuration parameter.
- **Approval by multi-factor authentication** is not set on the requested service item.

The process runs the `QER_CloudAssistant_CreateMessage_PWOHelperPWO` script passing to it the name and the UID of the adaptive card to send. The script created the adaptive card from the JSON template for adaptive cards and the data in the request and then sends it to the approver The `QER_CloudAssistant_CheckMessage_PWOHelperPWO` script checks if the approver has sent a response, evaluates the response and updates the request process according to the approval decision.

NOTE: If you want to use your own adaptive cards template, check the `QER_CloudAssistant_CreateMessage_PWOHelperPWO`, `QER_CloudAssistant_CreateData_PWOHelperPWO`, and `QER_CloudAssistant_CheckMessage_PWOHelperPWO` scripts and adjust them if necessary to reflect content changes in the template. For more information about overriding scripts, see the *One Identity Manager Configuration Guide*.

Related topics

- Creating, editing, and deleting adaptive cards templates for requests on page 200
- Creating, editing, and deleting adaptive cards for requests on page 198
- Using adaptive cards for approvals on page 196

Disabling adaptive cards

Adaptive cards that are not used can be disabled.

To disable an adaptive card

1. In the Manager, select the **IT Shop > Basic configuration data > Adaptive cards** category.
2. Select the adaptive card in the result list.
3. Select the **Change main data** task.
4. Set **Disabled**.
5. Save the changes.

Related topics

- Using adaptive cards for approvals on page 196
- Creating, editing, and deleting adaptive cards for requests on page 198
- General main data for adaptive cards on page 201

Requests with limited validity period for changed role memberships

If an identity changes their primary department (business role, cost center, or location), they lose all company resources and system entitlements inherited through it. However, it may be necessary for the identity to retain these company resources and system entitlements for a certain period. Use temporary requests to retain the state of the identity's current memberships. Inherited assignments are not removed until after the validity period for this request has expired. The identity can renew the request within the validity period.

Prerequisites

- Identity main data is modified by import.
- The import sets the session variable `FullSync=TRUE`.

To configure automatic requests for removal of role memberships

1. In the Designer, set the **QER | ITShop | ChallengeRoleRemoval** configuration parameter.
2. In the Designer, set the **QER | ITShop | ChallengeRoleRemoval | DayOfValidity** configuration parameter and enter a validity period for the request.
3. In the Designer, set the configuration parameters under **QER | ITShop | ChallengeRoleRemoval** for roles whose primary memberships need to remain intact when modified.
4. Commit the changes to the database.

NOTE: The configuration parameters are set by default. The validity period is set to seven days.

If identity main data is modified by importing, One Identity Manager checks if a primary role (for example `Person.UID_Department`) was modified or deleted on saving. If this is the case, `VI_CreateRequestForLostRoleMembership` is run. The script create a temporary assignment request for this role, which is granted approval automatically. Thus, the identity remains a members of the role and retains their company resources and system entitlements. The request is automatically canceled when the validity period expires.

The request can be renewed during the validity period. The request renewal must be approved by the role manager. The request becomes permanent if approval is granted. Role membership stays the same until the assignment is canceled.

TIP: The **QER | ITShop | ChallengeRoleRemoval | ITShopOrg** configuration parameter specifies which product nodes to use for a limited validity period request of modified role memberships. The **Challenge loss of role membership** product is available by default in the **Identity & Access Lifecycle | Identity Lifecycle** shelf. You can also add this product to your own IT Shop solution.

To use the "Challenge loss of role membership" product in your own IT Shop

1. Assign the **Challenge loss of role membership** assignment resource to one of your own shelves.
2. In the Designer, edit the value of the **QER | ITShop | ChallengeRoleRemoval | ITShopOrg** configuration parameter.
    - Enter the full name or the UID of the new product node.

Related topics

- Configuration parameters for the IT Shop on page 258

Requests from permanently deactivated identities

By default, permanently deactivated identities remain members in all the customer nodes. This ensures that all pending request and resulting assignments are retained.
One Identity Manager can be configured such that identities are automatically removed from all custom nodes once they are permanently deactivated. This means that all pending requests are broken off and remaining assignments are removed.

To remove identities from all customer nodes if they are permanently deactivated

- In the Designer, set the **QER | ITShop | AutoCloseInactivePerson** configuration parameter.

Deleting request procedures and deputizations

To limit request procedures in the One Identity Manager database, you can remove closed request procedures from the database. The request procedure properties are logged in the approval history at the same time. The requests are subsequently deleted. Only closed requests with unexpired retention periods are kept in the database.

If the request to be deleted still contains dependent requests, the request is only deleted after the dependent requests have been deleted. Dependent requests are requests that are entered into `PersonWantsOrg.UID_PersonWantsOrgParent`.

The same procedure is followed for completed deputizations. The properties of the deputizations are recorded; then the deputizations are deleted from the database.

To delete request procedures and deputizations automatically

1. In the Designer, set the **QER | ITShop | DeleteClosed** configuration parameter.
    a. To delete canceled requests, set the **QER | ITShop | DeleteClosed | Aborted** configuration parameter and set the retention period in days.
    b. To delete denied requests, set the **QER | ITShop | DeleteClosed | Dismissed** configuration parameter and set the retention period in days.
    c. To delete canceled requests, set the **QER | ITShop | DeleteClosed | Unsubscribed** configuration parameter and specify its retention period in days.
2. In the Designer, set the **Common | ProcessState | PropertyLog** configuration parameter and compile the database.

    If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

    The deleted deputizations, request procedures, and their approval history are logged. For more information about logging data changes, see the *One Identity Manager Configuration Guide*.

    NOTE: Ensure that the recorded request procedures and deputizations are archived for audit reasons. For more information about the archiving method, see the *One Identity Manager Data Archiving Administration Guide*.

Closed requests are deleted by the DBQueue Processor once the request's retention period has expired. As the basis for calculating the retention period, the request's cancellation date is used. If this date cannot be given, the time at which the request was last changed, is used. The DBQueue Processor determines the requests to be deleted in the context of daily maintenance tasks. All request procedure properties are logged in the approval history.

4

Managing an IT Shop

Depending on your company structure, you can use the supplied default shop, **Identity & Access Lifecycle**, extend it or set up your own IT Shop solution. Set up different IT Shop structures for your custom IT Shop solution. Specify which identities are authorized to make request in the shops.

To set up an IT Shop solution with the help of the IT Shop wizard.

- In the Manager, select the **My One Identity Manager > IT Shop wizards > Create shop** category.

  The wizard includes the most important configuration stages for setting up an IT Shop. After completing the wizard, there may be other configuration steps necessary.

IT Shop structures such as shopping centers, shops, and shelves are mapped in the **IT Shop > IT Shop** category. An IT Shop solution is displayed hierarchically.

The following sections describe the procedure for manually setting up an IT Shop.

IT Shop base data

Various base data is required to construct an IT Shop:

- Processing status

  Processes statuses pass on the status of single approval steps. You can set the processing status for each approval step in the approval workflow depending on whether the approval decision was negative or positive. Depending on the result of the approval decision, the appropriate processing status is set for the request.

  For more information, see Processing status on page 208.

- Standard reasons

  Standard reasons are predefined reasons that can be selected in the Web Portal when making approval decisions.

  For more information, see Standard reason for requests on page 209.

- Approval policies

  One Identity Manager uses approval policies to determine the approver for each request process.

  For more information, see Approval policies for requests on page 85.

- Approval workflows

  Approval workflows define all the necessary steps for making approval decisions for request processes.

  For more information, see Approval workflows for requests on page 90.

- Approval procedure

  Approval procedures are used to find the approvers required for an approval step.

  For more information, see Setting up approval procedures on page 125.

- Mail templates

  Mail templates are used to send email messages to requesters and approvers.

  For more information, see Custom mail templates for notifications on page 243.

- Adaptive cards

  To allow approvers who temporarily do not have access to the One Identity Manager tools to approve requests, you can send adaptive cards.

  For more information, see Creating, editing, and deleting adaptive cards for requests on page 198.

- Role classes

  Use role classes to specify which company resources can be requested through the IT Shop. At the same time, you decide which company resources may be assigned as products to shelves and IT Shop templates.

  For more information, see Role classes for the IT Shop on page 211.

- Role types

  Role types are used to group roles into a role class. Within the IT Shop, role types can e used to group shop and to restrict the effective approval policies for a shelf.

  For more information, see Role types for the IT Shop on page 212.

- Business Partners

  In One Identity Manager, you can enter the data for external businesses that could be act as manufacturers, suppliers, or partners. You assign a manufacturer to a service item.

  For more information, see Business partners on page 212.

- Functional areas

  To analyze rule checks for different areas of your company in the context of identity audit, you can set up functional areas. Moreover, functional areas can be replaced by peer group analysis during request approvals or attestation cases. Functional areas can be assigned to service items.

For more information, see Functional areas on page 214.

- Service categories

  Service categories are used to group service items and make them available in the Web Portal.

  For more information, see Entering service categories on page 36.

- Tags

  Product owners are able to add tags to their products. These tags can be used as search criteria by requests in the Web Portal.

  For more information, see Entering tags on page 52.

- Request properties

  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.

  For more information, see Entering product-specific request properties on page 40.

- Chief approval team

  There is a default application role in One Identity Manager for the chief approval team. Assign identities to this application role, who are authorized to approve, deny, cancel requests, or to authorize other approvers in special cases.

  For more information, see Chief approval team on page 215.

- Product owners

  A default application role for product owners is available in One Identity Manager. Assign the identities to this application role, who are authorized to approve requests and edit the main data of service items or service categories.

  For more information, see Product owners on page 216.

- Attestors

  A default application role for attestors is available in One Identity Manager. Assign the identities to this application role, who are authorized to attest IT Shop structures.

  For more information, see Attestors on page 217.

Processing status

Processes statuses pass on the status of single approval steps. You can set the processing status for each approval step in the approval workflow depending on whether the approval decision was negative or positive. Depending on the result of the approval decision, the appropriate processing status is set for the request.

To edit processing statuses

1. In the Manager, select the **IT Shop > Basic configuration data > Processing status** category.
2. In the result list, select a processing status and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the processing status's main data.
4. Save the changes.

Enter the following properties for a processing status.

Table 54: General main data of a processing status

Property	Description
Processing status	Name of the processing status.
Success	The processing status marks the success of the processing step.
Closed	The processing status marks whether processing is complete.
Sort order	Order in which processing status can be set.
Description	Text field for additional explanation.

Related topics

- Properties of an approval step on page 95

Standard reason for requests

For requests or the approval of requests, you can specify reasons in the Web Portal that explain the request sequence and the individual approval decisions. You can freely formulate this text. You also have the option to predefine reasons. The approvers can select a suitable text from these standard reasons in the Web Portal and store it with the request.

Standard reasons are displayed in the approval history and the request details.

To create or edit standard reasons

1. In the Manager, select the **IT Shop > Basic configuration data > Standard reasons** category.
2. Select a standard reason in the result list and run the **Change main data** task.

   - OR -

   Click in the result list.

3. Edit the main data of a standard reason.
4. Save the changes.

Enter the following properties for the standard reason.

Table 55: General main data of a standard reason

Property	Description
Standard reason	Reason text as displayed in the Web Portal and in the approval history.
Description	Text field for additional explanation.
Automatic Approval	Specifies whether the reason text is only used for automatic approvals by One Identity Manager. This standard reason cannot be selected by manual approvals in the Web Portal. Do not set the option if the you want to select the standard reason in the Web Portal.
Additional text required	Specifies whether an additional reason should be entered in free text for the approval.
Usage type	Usage type of standard reason. Assign one or more usage types to allow filtering of the standard reasons in the Web Portal.

Related topics

- Predefined standard reasons for requests on page 210

Predefined standard reasons for requests

One Identity Manager provides predefined standard reasons. These are added to the request by One Identity Manager during automatic approval. You can use the usage type to specify which standard reasons can be selected in the Web Portal.

To change the usage type

1. In the Manager, select the **IT Shop > Basic configuration data > Standard reasons > Predefined** category.
2. Select the standard reason whose usage type you want to change.
3. Select the **Change main data** task.
4. In the **Usage type** menu, set all the actions where you want to display the standard reason in the Web Portal.

   Unset all the actions where you do not want to display the default reason.
5. Save the changes.

Related topics

- Standard reason for requests on page 209

Role classes for the IT Shop

Role classes form the basis for mapping IT Shop structures in One Identity Manager. The following role classes are available by default in One Identity Manager:

- IT Shop structure
- IT Shop template (if the **QER | ITShop | Templates** configuration parameter is set)

Use role classes to specify which company resources can be requested through the IT Shop. At the same time, you decide which company resources may be assigned as products to shelves and IT Shop templates.

The following options define which company resources may be assigned to IT Shop structures and IT Shop templates:

- Assignments allowed

  This option specifies whether the assignment of the relevant company resources is permitted in general.

- Direct assignments allowed

  This option specifies whether the relevant company resources can be directly assigned.

NOTE: Company resources are always assigned directly to shelves and IT Shop templates. Therefore, always enable and disable both options.

To configure assignment to IT Shop structures and IT Shop templates

1. In the Manager, select the **IT Shop > Basic configuration data > Role classes** category.
2. In the result list, select the role class.
3. Select the **Configure role assignments** task.
4. In the **Role assignments** column, select a company resource.

   Enable the **Assignments permitted** option, to specify whether an assignment is generally allowed.

   Enable the **Direct assignment permitted** options, to specify whether a direct assignment is allowed.

   Disable the options if the assignment is not allowed.

   INFORMATION: You can only disable the options if there are no assignments of the respective objects to IT Shop structures or IT Shop templates.
5. Save the changes.

Role types for the IT Shop

Create role types in order to classify roles. You can use role types to limit the approval policies in effect for shelves. To do this, assign role types to shelves and approval policies.

You can also assign role types to shops if you want to apply further criteria to distinguish between shops. Role types for shops do not, however, influence how the approval policies in effect are determined.

To edit a role type

1. In the Manager, select the **IT Shop > Basic configuration data > Role types** category.
2. In the result list, select the role type and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Enter a name and detailed description for the role type.
4. Save the changes.

Related topics

- Determining effective approval policies on page 103

Business partners

In One Identity Manager, you can enter the data for external businesses that could be act as manufacturers, suppliers, or partners. You assign a manufacturer to a service item.

To edit business partners

1. In the Manager, select the **IT Shop > Basic configuration data > Business partners** category.
2. In the result list, select a business partner and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the business partner's main data.
4. Save the changes.

Enter the following data for a company.

Table 56: General main data of a company

Property	Description
Company	Short description of the company for the views in One Identity Manager tools.
Name	Full company name.
Surname prefix	Additional company name.
Short name	Company's short name.
Contact	Contact person for the company.
Partner	Specifies whether this is a partner company.
Customer number	Customer number at the partner company.
Supplier	Specifies whether this is a supplier.
Customer number	Customers number at supplier.
Leasing partner	Specifies whether this is a leasing provider or rental firm.
Manufacturer	Specifies whether this is a manufacturer.
Remarks	Text field for additional explanation.

Table 57: Company address

Property	Description
Street	Street or road.
Building	Building
Zip code	Zip code.
City	City.
State	State.
Country	Country.
Phone	Company's telephone number.
Fax	Company's fax number.
Email address	Company's email address.
Website	Company's website. Click the button to display the web page in the default web browser.

Functional areas

To analyze rule checks for different areas of your company in the context of identity audit, you can set up functional areas. Assign functional areas to hierarchical roles, compliance rules, SAP functions, and service items. Enter criteria for the functional areas and hierarchical roles that provide information about the risk level of rule violations. To assess the risks, specify how many rule violations are permitted in a functional area or role. You can enter separate assessment criteria for each role, such as a risk index or transparency index.

Moreover, functional areas can be replaced by peer group analysis during request approvals or attestation cases.

Example: Use of functional areas

To assess the risk of rule violations for service items. Proceed as follows:

1. Set up functional areas.
2. Assign service items to the functional areas.
3. Specify the number of rule violations allowed for the functional area.
4. Assign the functional areas to the compliance rules that are relevant for the assessment.
5. Use the One Identity Manager report function to create a report that prepares the result of rule checking for the functional area by any criteria.

To create or edit a functional area

1. In the Manager, select the **IT Shop > Basic configuration data > Functional areas** category.
2. In the result list, select a function area and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the function area main data.
4. Save the changes.

Enter the following data for a functional area.

Table 58: Functional area properties

Property	Description
Functional area	Description of the functional area
Parent Functional	Parent functional area in a hierarchy.

Property	Description
area	Select a parent functional area from the list for organizing your functional areas hierarchically.
Max. number of rule violations	List of rule violation valid for this functional area. This value can be evaluated during the rule check. NOTE: This property is available if the Compliance Rules Module is installed.
Description	Text field for additional explanation.

Related topics

- Approval by peer group analysis on page 147

Chief approval team

Sometimes, approval decisions cannot be made for requests because the approver is not available or does not have access to One Identity Manager tools. To complete these requests, you can define a chief approval team whose members are authorized to intervene in the approval process at any time.

There is a default application role in One Identity Manager for the chief approval team. Assign this application role to all identities who are authorized to approve, deny, cancel requests in special cases, or to authorize other approvers. For more information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 59: Default application role for chief approval team

User	Tasks
Chief approval team	Chief approvers must be assigned to the **Request & Fulfillment | IT Shop | Chief approval team** application role. Users with this application role: • Approve through requests. • Assign requests to other approvers.

To add members to the chief approval team

1. In the Manager, select the **IT Shop > Basic configuration data > Chief approval team** category.
2. Select the **Assign identities** task.

   In the **Add assignments** pane, assign the identities who are authorized to approve all requests.

   TIP: In the **Remove assignments** pane, you can remove assigned identities.

To remove an assignment

- Select the identity and double-click ✓.

3. Save the changes.

Detailed information about this topic

- Approval by the chief approval team on page 161

Product owners

Identities who are approvers in approval processes for requesting service items can be assigned to these service items. To do this, assign a service item or a service category to an application role for **Product owners**. Assign identities to this application role who are authorized to approve requests in the IT Shop and to edit service item or service category main data.

A default application role for product owners is available in One Identity Manager. You may create other application roles as required. For more information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 60: Default application roles for product owners

User	Tasks
Product owners	Product owners must be assigned to the **Request & Fulfillment | IT Shop | Product owners** application role or a child application role. Users with this application role: • Approve through requests. • Edit service items and service categories under their management.

To add identities to the default application role for product owners

1. In the Manager, select the **IT Shop > Basic configuration data > Product owners** category.
2. Select the **Assign identities** task.

   In the **Add assignments** pane, add identities.

   TIP: In the **Remove assignments** pane, you can remove assigned identities.

   To remove an assignment

   - Select the identity and double-click ✓.

3. Save the changes.

To add another application role for product owners

1. In the Manager, select the **IT Shop > Basic configuration data > Product owners** category.
2. Click in the result list.
3. Enter at least the application role's name and, in the **Parent application role** drop-down, select the **Request & Fulfillment | IT Shop | Product owners** application role or a child role.
4. Save the changes.
5. Assign identities to the application role.

Related topics

- Deleting unused application roles for product owners on page 83

Attestors

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

In One Identity Manager, you can assign identities, who are brought in as attestors to attest these objects, to IT Shop structures (shelves, shops, shopping centers, service categories, and shelf templates). To do this, assign the IT Shop structures to application roles for attestors. Assign these application roles to identities who are authorized to attest these objects and their assignments.

For more information about attestation, see the *One Identity Manager Attestation Administration Guide*.

A default application role for attestors is available in One Identity Manager. You may create other application roles as required. For more information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 61: Default application roles for attestors

User	Tasks
Attestors for IT Shop	Attestors must be assigned to the **Request & Fulfillment | IT Shop | Attestors** application role. Users with this application role: • Attest correct assignment of company resource to IT Shop structures for which they are responsible. • Attest objects that have service items assigned to them. • Can view main data for these IT Shop structures but not edit them. NOTE: This application role is available if the Attestation Module is installed.

To add identities to default application roles for attestors

1. In the Manager, select the **IT Shop > Basic configuration data > Attestors** category.
2. Select the **Assign identities** task.

   In the **Add assignments** pane, add identities.

   TIP: In the **Remove assignments** pane, you can remove assigned identities.

   To remove an assignment

   - Select the identity and double-click .
3. Save the changes.

To add another application role for attestors

1. In the Manager, select the **IT Shop > Basic configuration data > Attestors** category.
2. Click in the result list.
3. Enter at least the application role's name and, in the **Parent application role** drop-down, select the **Request & Fulfillment | IT Shop | Attestor** application role or a child role.
4. Save the changes.
5. Assign identities to the application role.

Related topics

- General main data for service items on page 23
- Main data for service categories on page 36
- General main data of IT Shop structures on page 219
- General main data of a shelf template on page 237

Setting up IT Shop structures

Depending on the company structure, you can optionally define shopping centers for your IT Shop solution where several shops can be bought together under one roof. Always add the shopping center to the top level of the IT Shop. Shopping centers may not be hierarchical.

Each shop contains a number of shelves that the customer can request products from. You can add a shop to the top level of the IT Shop or under a shopping center. Shops may not be hierarchical.

There are various products available for request on shelves. Shelves are set up under each shop.

IMPORTANT: If a shop contains a large number of customers, the calculations in the IT Shop can cause a heavy load on the DBQueue Processor and therefore on the database server, as well.

Structure the IT Shop so that no more than 30,000 customers can make requests in each shop. If necessary, set up your own shopping center with several shops and customer nodes.

Detailed information about this topic

- Adding IT Shop structures on page 219
- Deleting IT Shop structures on page 228

Adding IT Shop structures

To set up a shopping center, a shop or a shelf

1. In the Manager, select the **IT Shop > IT Shop** category.
2. Click in the result list.
3. Edit the shopping center, shop, or shelf's main data.
4. Save the changes.

Detailed information about this topic

- General main data of IT Shop structures on page 219
- Custom main data of IT Shop structures on page 221

General main data of IT Shop structures

On the **General** tab, enter the following main data of a shopping center, shop, or a shelf.

Table 62: General main data of an IT Shop structure

Property	Description
IT Shop node	IT Shop structure name.
Internal name	Internal IT Shop structure name.
IT Shop information	The structure of the IT Shop is governed by this data The IT Shop structure is regulated by this data. In the drop-down, select **Shopping center**, **Shop**, or **Shelf**. The menu is only displayed when you insert a new IT Shop structure.

Property	Description
Role type	Role types for classifying shops and shelves. In the menu, select a role type. • Shopping center: N/A • Shop: You can use role types to classify shops further. The role type for shops does not influence how the approval policies in effect are determined. • Shelf: You can use role types to limit the approval policies in effect.
Shelf template	Template to automatically fill shelves. • Shopping center: Select a shopping center template from the menu. A shopping center template cannot be assigned until the shopping center has been saved in the database. • Shop: N/A • Shelf: For shelves created by automatic filling of the shop, the reference to the shelf template used is entered. Shelf templates are only assigned automatically.
Parent IT Shop node	Parent IT Shop nodes in the IT Shop hierarchy. • Shopping center: Leave this empty. Shopping centers always form the root node of an IT Shop. • Shop: If the shop is at the top level of an IT Shop, this field stays empty. If the shop is in a shopping center, select the shopping center from the menu. You can use this input field to add shops to shopping centers later. • Shelf: In the menu, select the shop to add the shelf to. After saving the rule, the shop cannot be changed again.
Full name	Full name of the IT Shop structure.
Location	Location of the IT Shop structure. You can use this input when creating approval policies for making requests from this shopping center/shop/shelf.
Department	Department the IT Shop structure is in. You can use this input when creating approval policies for making requests from this shopping center/shop/shelf.
Cost center	Cost enter of the IT Shop structure. You can use this input when creating approval policies for making requests from this shopping center/shop/shelf.
Owner	The identity responsible for the IT Shop structure. You can use this input

Property	Description
	when creating approval policies for making requests from this shopping center/shop/shelf.
2nd Manager	The owner's deputy. You can use this input when creating approval policies for making requests from this shopping center/shop/shelf.
Attestors	Applications role whose members are authorized to approve attestation cases for this IT Shop structure. To create a new application role, click . Enter the application role name and assign a parent application role. NOTE: This property is available if the Attestation Module is installed.
Description	Text field for additional explanation.
Certification status	Certification status of the IT Shop structure. You can select the following certification statuses: • **New**: The IT Shop structure was newly added to the One Identity Manager database. • **Certified**: The IT Shop structure's main data was granted approval by the manager. • **Denied**: The IT Shop structure's main data was denied approval by the manager.

Detailed information about this topic

- Role types for the IT Shop on page 212
- Templates for automatically filling the IT Shop on page 232
- Attestors on page 217

Related topics

- Determining effective approval policies on page 103

Custom main data of IT Shop structures

Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Assigning approval policies

You can assign approval policies to a shopping center, shops, and shelves. These are applied to all request from this IT Shop structure if a child IT Shop structure or the requested service items are not assigned to approval policies. The approval policy that takes effect on the IT Shop structure is shown in the overview.

To assign an IT Shop structure to an approval policy.

1. In the Manager, select the **IT Shop > IT Shop** or the **IT Shop > IT Shop > <IT Shop structure>** category.
2. Select the IT Shop structure in the result list.
3. Select the **Assign approval policies** task.

   In the **Add assignments** pane, assign the approval policies.

   TIP: In the **Remove assignments** pane, you can remove approval policy assignments.

   To remove an assignment

   - Select the approval policy and double-click .
4. Save the changes.

Related topics

- Approval processes for IT Shop requests on page 85

Assigning requestable products to shelves

Assign a shelf those company resources that the shop customers are permitted to request as products. These company resources are added as product nodes below the shelf. You can only select those company resources that are labeled with the **IT Shop** option and to which a service item is assigned.

To assign company resources, select one of the tasks in the task view. The tasks are only shown if the **Assignments permitted** and **Direct assignment permitted** options are enabled for the **IT Shop structure** role class.

To assign company resources as products to a shelf

1. In the Manager, select the **IT Shop > IT Shop > <shop>** category or the **IT Shop > IT Shop > <shopping center> > <shop>** category.
2. Select the shelf in the result list.
3. Select the **Assign <company resource>** task.

   In the **Add assignments** pane, assign company resources..

TIP: In the **Remove assignments** pane, you can remove company assignments.

To remove an assignment

- Select the company resource and double-click ✓.

4. Save the changes.

Related topics

- Preparing products for requesting on page 21
- Assigning and removing products on page 54
- Role classes for the IT Shop on page 211

The IT Shop structure overview

To obtain an overview of a shopping center

1. In the Manager, select the **IT Shop > IT Shop** category.
2. Select the shopping center template in the result list.
3. Select the **Shopping center overview** task.

To obtain an overview of a shop

1. In the Manager, select the **IT Shop > IT Shop** or the **IT Shop > IT Shop > <shopping center>** category.
2. Select the shop in the result list.
3. Select the **Shop overview** task.

To obtain an overview of a shelf

1. In the Manager, select the **IT Shop > IT Shop > <shop>** category or the **IT Shop > IT Shop > <shopping center> > <shop>** category.
2. Select the shelf in the result list.
3. Select the **Shelf overview** task.

Setting up a customer node

Set up only one customer node for each shop to facilitate customer administration. Add the identities to this customer node who are permitted to request products from this shop.

IMPORTANT: If a shop contains a large number of customers, the calculations in the IT Shop can cause a heavy load on the DBQueue Processor and therefore on the database server, as well.

Ensure that no more than 30,000 identities are members in a customer node. If necessary, set up your own shopping center with several shops and customer nodes.

Adding customer nodes

To set up a customer node

1. In the Manager, select the **IT Shop > IT Shop > <shop>** category or the **IT Shop > IT Shop > <shopping center> > <shop>** category.
2. Click in the result list.
3. Edit the customer node's main data.
4. Save the changes.

General main data of customer nodes

Enter the following main data of a customer node:

Table 63: General main data of a customer node

Property	Description
IT Shop node	IT Shop structure name.
Internal name	Internal IT Shop structure name.
IT Shop information	Labels the IT Shop structure as customer node. In the drop-down, select **`Customers`**. The drop-down is only displayed when you insert a new IT Shop structure.
Role type	Not relevant
Shelf template	N/A.
Parent IT Shop node	Parent IT Shop nodes in the IT Shop hierarchy. Select the shop to which the customer node will be added. Only one customer node is allowed per shop.
Full name	Full identifier of the customer node.
Location	N/A.
Department	N/A.
Cost center	N/A.

Property	Description
Owner	N/A.
Deputy manager	N/A.
Attestors	N/A.
Description	Text field for additional explanation.
Dynamic roles not allowed	Specifies whether a dynamic role can be created for the customer node.

Related topics

- Assigning identities through dynamic roles on page 226

Custom main data of customer nodes

Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Assigning identities directly

Add an identity that is authorized to make requests for the shop to the customer node. You have two possible ways of doing this. Identities can be assigned to a customer node either directly or through a dynamic role.

IMPORTANT: If a shop contains a large number of customers, the calculations in the IT Shop can cause a heavy load on the DBQueue Processor and therefore on the database server, as well.

Never assign more than 30,000 identities to a customer node.

To assign identities directly to a custom node

1. In the Manager, select the **IT Shop > IT Shop > <shop> > Customers** category or the **IT Shop > IT Shop > <shopping center> > <shop> > Customers** category.
2. Select the **Assign identities** task.

   In the **Add assignments** pane, assign the identities authorized to make requests.

   TIP: In the **Remove assignments** pane, you can remove assigned identities.

To remove an assignment

- Select the identity and double-click ✓.

3. Save the changes.

If an identity is removed from a customer node, all pending requests for this identity are canceled.

Related topics

- Assigning identities through dynamic roles on page 226

Assigning identities through dynamic roles

Add an identity that is authorized to make requests for the shop to the customer node. You have two possible ways of doing this. Identities can be assigned to a customer node either directly or through a dynamic role.

NOTE: **Create dynamic role** is only available for customer nodes that do not have **Dynamic roles not allowed** set.

IMPORTANT: If a shop contains a large number of customers, the calculations in the IT Shop can cause a heavy load on the DBQueue Processor and therefore on the database server, as well.

Formulate the condition for the dynamic role so that no more than 30,000 identities are found.

To create a dynamic role

1. In the Manager, select the **IT Shop > IT Shop > <shop> > Customers** category or the **IT Shop > IT Shop > <shopping center> > <shop> > Customers** category.
2. Select the **Create dynamic role** task.
3. Enter the required main data.
4. Save the changes.

To edit a dynamic role

1. In the Manager, select the **IT Shop > IT Shop > <shop> > Customers** category or the **IT Shop > IT Shop > <shopping center> > <shop> > Customers** category.
2. Select the **Entitled customers overview** task.
3. Select the **Dynamic roles** form element and click on the dynamic role.
4. Select the **Change main data** task and edit the dynamic role's main data.
5. Save the changes.

For more information about dynamic roles, see the *One Identity Manager Identity Management Base Module Administration Guide*. The following features apply to dynamic roles for customer nodes:

Table 64: Properties of a customer node dynamic role

Property	Description
IT Shop node	This data is initialized with selected customer nodes. If the identities meet the dynamic role conditions, they are added to this customer node.
Object class	Employee
Dynamic role	The dynamic role name is made up of the object class and the full name of the IT Shop node by default.
Calculation schedule	Schedule for calculating dynamic roles. Identities with request permissions for the shop are determined regularly at the times specified in the schedule. In the default installation of One Identity Manager, the **Dynamic roles check** schedule is already defined. All dynamic role memberships are checked using this schedule and recalculation operations are sent to the DBQueue Processor if necessary. Use the Designer to customize schedules or set up new ones to meet your requirements. For more information, see the *One Identity Manager Operational Guide*.

To delete a dynamic role

1. In the Manager, select the **IT Shop > IT Shop > <shop> > Customers** category or the **IT Shop > IT Shop > <shopping center> > <shop> > Customers** category.
2. Select the **Entitled customers overview** task.
3. Select the **Dynamic roles** form element and click on the dynamic role.
4. In the Manager's toolbar, click .
5. Confirm the security prompt with **Yes**.

Related topics

- Assigning identities directly on page 225

The entitled customers overview

To obtain an overview of a customer node

1. In the Manager, select the **IT Shop > IT Shop > <shop> > Customers** category or the **IT Shop > IT Shop > <shopping center> > <shop> > Customers**

category.

2. Select the **Entitled customers overview** task.

Deleting IT Shop structures

In order to delete IT Shop structures, you have to remove all the child IT Shop structures. This applies to manually added IT Shop structures in the same way as it does for shelves and products created from shelf templates.

Detailed information about this topic

- Deleting customer nodes on page 228
- Deleting shelves on page 228
- Deleting shops on page 229
- Deleting shopping centers on page 230

Deleting customer nodes

To delete a customer node

1. In the Manager, select the **IT Shop > IT Shop > <shop>** category or the **IT Shop > IT Shop > <shopping center> > <shop>** category.
2. Select the customer node in the result list.
3. Remove all assigned identities.
    - If the customer node was filled using a dynamic role, delete the dynamic role first.
4. Click in the result list.
5. Confirm the security prompt with **Yes**.

Detailed information about this topic

- Assigning identities directly on page 225
- Assigning identities through dynamic roles on page 226

Deleting shelves

If a shelf is going to be completely dissolved, you need to remove all the product assignments from the shelf first.

To delete a shelf

1. In the Manager, select the **IT Shop > IT Shop > <shop>** category or the **IT Shop > IT Shop > <shopping center> > <shop>** category.
2. Select the shelf in the result list.
3. Remove all product assignments to the shelf.

   The next time the DBQueue Processor runs, all pending requests for the products are closed and approved requests are canceled. Then you can delete the shelf.
4. Click in the result list.
5. Confirm the security prompt with **Yes**.

To delete a shelf that resulted from a special shelf template

1. Cancel approved requests from this shelf.
2. Cancel pending request.
3. Remove shelf template assignments to the shop.

NOTE: Shelves that have been created from a global shelf template or a shopping center template cannot be deleted.

Detailed information about this topic

- Removing products from shelves on page 57
- Assigning shelf templates to shops and shopping center templates on page 240

Deleting shops

If you want to delete a shop, delete the customer node and existing shelves beforehand.

To delete a shop

1. In the Manager, select the **IT Shop > IT Shop** or the **IT Shop > IT Shop > <shopping center>** category.
2. Select the shop in the result list.
3. Delete the customer node.
4. Delete all shelves.
5. Click in the result list.
6. Confirm the security prompt with **Yes**.

Detailed information about this topic

- Deleting customer nodes on page 228
- Deleting shelves on page 228

Deleting shopping centers

If you want to delete a shopping center, delete all shops first.

To delete a shopping center

1. In the Manager, select the **IT Shop > IT Shop** category.
2. Select the shopping center template in the result list.
3. Delete all shops.
4. Click in the result list.
5. Confirm the security prompt with **Yes**.

Detailed information about this topic

- Deleting shops on page 229

Restructuring the IT Shop

If necessary, custom IT Shop structures can be reorganized by moving stores, shelves, or products to other IT Shop structures. In the Manager, you can use the following tasks to do this:

- Shop: Move to another shopping center
- Shelf: Move to another shop
- Shelf: Move products to another shelf
- Shelf: Move to another shelf

If products that already have requests are moved to another shop, verification is carried out to ascertain whether the request recipient is also a customer in the new shop.

NOTE: Default IT Shop structures cannot be moved.

Detailed information about this topic

- Moving products to another shelf on page 231
- Moving shops to other shopping centers on page 231
- Moving shelves to other shops on page 231
- Product request on customer or product relocation on page 49

Moving shops to other shopping centers

NOTE: Default shops cannot be moved.

To move a shop to another shopping center

1. In the Manager, select the **IT Shop > IT Shop** or the **IT Shop > IT Shop > <shopping center>** category.
2. Select the shop in the result list.
3. Select the **Move to another shopping center** task.
4. Select the shopping center to move the shop to.
5. Click **OK**.

Related topics

- Product request on customer or product relocation on page 49
- Restructuring the IT Shop on page 230

Moving shelves to other shops

NOTE: Default shelves cannot be moved.

To move a shelf to another shop

1. In the Manager, select the **IT Shop > IT Shop > <shop>** category or the **IT Shop > IT Shop > <shopping center> > <shop>** category.
2. Select the shelf in the result list.
3. Select the **Move to another shop** task.
4. Select the shop to move the shelf to.
5. Click **OK**.

Related topics

- Product request on customer or product relocation on page 49
- Restructuring the IT Shop on page 230

Moving products to another shelf

A product can be moved to another shelf. If the shelf is in another shop, the system checks whether the request recipient is also a customer in the new shop.

NOTE: Standard products cannot be moved.

To move a product to another shelf

1. In the Manager, select the **IT Shop > IT Shop > <shop> > Shelf: <shelf>** or the **IT Shop > IT Shop > <shopping center> > <shop> > Shelf: <shelf>** category.
2. Select an object in the result list.
3. Select the **Move to another shelf** task.
4. Select the new shelf.
5. Click **OK**.

To move multiple products to another shelf

1. In the Manager, select the **IT Shop > IT Shop > <shop>** category or the **IT Shop > IT Shop > <shopping center> > <shop>** category.
2. Select the shelf in the result list.
3. Select the **Move products to another shelf** task.
4. Select the shelf to move the products to.
5. Select which products to move.
6. Click **OK**.

Detailed information about this topic

- Product request on customer or product relocation on page 49
- Restructuring the IT Shop on page 230

Templates for automatically filling the IT Shop

You can create templates for setting up shelves automatically. Use templates when you want to set up shelves in several shops or shopping centers with the same products.

Table 65: Templates overview

Template	Description
Global shelf templates	A global shelf template is automatically distributed to all shops within the IT Shop solution. A corresponding shelf with products is added to each shop. If a new shop is created within the IT Shop solution, the global shelf template is immediately applied to the shop. NOTE: Global shelf templates are not distributed to default shops.

Template	Description
Special shelf templates	A special shelf template is manually assigned to one or more shops. A corresponding shelf with products is added in these shops. A special template can be distributed additionally to shopping center templates.
Shopping center templates	A shopping center template references one or more shopping centers. You can only assign shopping center template to shopping center. Once you assign a special shelf template to a shopping center template, a corresponding shelf is added to all the shops in the shopping center.

In order to simplify understanding, these templates are given the umbrella term **shelf templates** in the following.

To use shelf templates

- In the Designer, set the **QER | ITShop | Templates** configuration parameter.

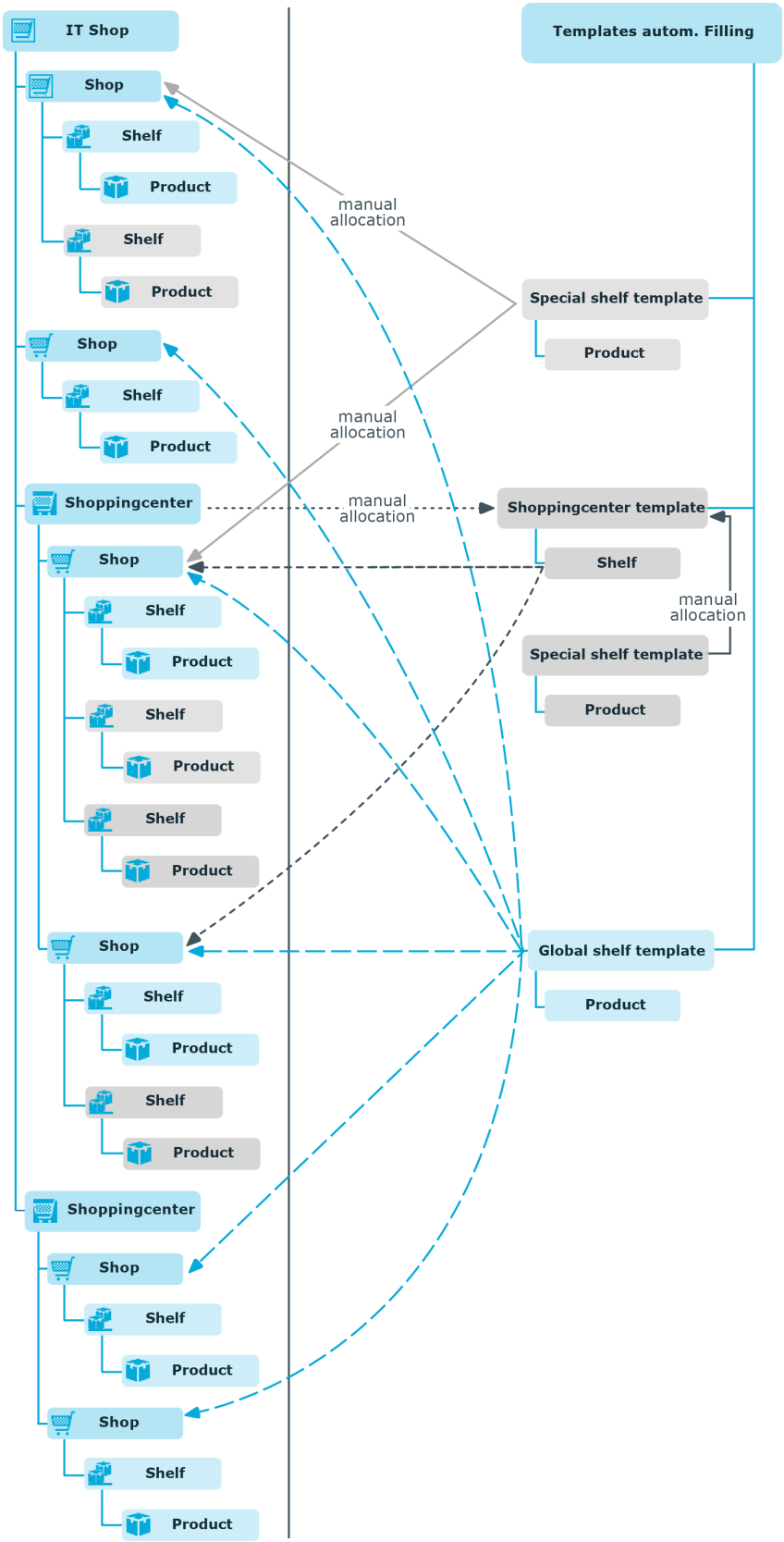
  NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

The following is valid for all shelf templates:

- If a template is modified, the changes are passed on to all shelves created from this shelf template.
- If a shelf template is deleted, all the shelves that originated from it are deleted from the shop. Outstanding requests are completed.
- Shelf templates can only be deleted when their assigned products and approval policies have been removed.

The following diagram illustrates the shelf templates that can be set up, their assignments, and the resulting IT Shop solution.

Figure 11: Assigning shelf templates


IT Shop
Templates autom. Filling
Shop
Shelf
Product
Shelf
Product
manual allocation
Special shelf template
Product
Shop
Shelf
Product
manual allocation
Shoppingcenter
manual allocation
Shoppingcenter template
Shop
Shelf
Shelf
Product
manual allocation
Special shelf template
Shelf
Product
Product
Shelf
Product
Shelf
Product
Shop
Global shelf template
Shelf
Product
Product
Shelf
Product
Shoppingcenter
Shop
Shelf
Product
Shop
Shelf
Product

Using shelf templates in an IT Shop solution

To create different shelf templates and implements in an IT Shop solution, do the following:

Global shelf templates

1. Create a global shelf template.
2. Assign products and approval policies to global shelf template.

The global shelf template is automatically reproduced in all shops in IT Shop. The shelves that created are linked to the global shelf template from which they originate. The products are transferred from the template to the shelf that is created from the template.

NOTE: Global shelf templates are not distributed to default shops.

Special shelf template

1. Create a special shelf template.
2. Assign products and approval policies to the special shelf template.
3. Assign the special shelf template to one or more shops.

The special shelf template is automatically copied to all shops in the IT Shop. The shelves that created are linked to the special shelf template from which they originate. The products are transferred from the template to the shelf that is created from the template.

Shopping center template

1. Create a shopping center template.
2. Create a special shelf template.
3. Assign products and approval policies to the special shelf template.
4. Assign the special shelf template to the shop center template.
5. Assign the shopping center template to the desired shopping centers.

The special shelf template is automatically copied to the shopping center template. Subsequently, the shelf created form the shopping center template is distributed to all the shops in the shopping center. The shelves that are created obtain a link to the shelf that they originated from.

Detailed information about this topic

- Editing shelf templates on page 237
- Assigning approval policies on page 238
- Assigning requestable products to shelf templates on page 239
- Shelf-filling wizard on page 240
- Assigning shelf templates to shops and shopping center templates on page 240
- General main data of IT Shop structures on page 219

Editing shelf templates

To edit a shelf template

1. In the Manager, select the **IT Shop > Shelf templates** category.
2. In the result list, select a mail template in and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the shelf template's main data.
4. Save the changes.

General main data of a shelf template

Enter the following properties for a shelf template.

Table 66: General main data of a shelf template

Property	Description
IT Shop node	Identifier of the IT Shop structure for creating the shelf template.
Internal name	Internal name of the shelf template.
IT Shop information	Type of shelf template. In the drop-down, select **`Shopping center template`**, **`Global shelf template`**, or **`Shelf template`**.
Role type	Role types for classifying shops and shelves. In the drop-down, select a role type. • Shopping center template: N/A • Global and special templates: You can use role types to limit the approval policies in effect. The role type is applied to the new shelf.
Location	Location of the shelf. You can use this data in approval workflows for determining the approver responsible for requests from the shelves that have been created.
Department	Department the shelf belongs to. You can use this data in approval workflows for determining the approver responsible for requests from the shelves that have been created.
Cost center	Cost center of the shelf. You can use this data in approval workflows for determining the approver responsible for requests from the shelves that have been created.
Owner	Identity responsible for the shelf. You can use this data in approval

Property	Description
	workflows for determining the approver responsible for requests from the shelves that have been created.
Deputy manager	The owner's deputy. You can use this data in approval workflows for determining the approver responsible for requests from the shelves that have been created.
Attestors	Applications role whose members are authorized to approve attestation cases for this business role. To create a new application role, click . Enter the application role name and assign a parent application role. NOTE:This property is available if the Attestation Module is installed.
Description	Text field for additional explanation.
Certification status	The shelf template's certification status. You can select the following certification statuses: • **New**: The shelf template was newly added to the One Identity Manager database. • **Certified**: A manager granted approval to the shelf template's main data. • **Denied**: A manager denied approval to the shelf template's main data.

Detailed information about this topic

- Role types for the IT Shop on page 212
- Attestors on page 217

Related topics

- Determining effective approval policies on page 103

Custom main data of shelf templates

Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Assigning approval policies

You can assign approval policies to global and special templates. These approval policies are passed on to every new shelf.

To assign a shelf template to an approval policy

1. In the Manager, select the **IT Shop > Shelf templates** category.
2. Select the rule template in the result list.
3. Select the **Assign approval policies** task.

   In the **Add assignments** pane, assign the approval policies.

   TIP: In the **Remove assignments** pane, you can remove approval policy assignments.

   To remove an assignment

   - Select the approval policy and double-click ✓.
4. Save the changes.

Related topics

- Approval processes for IT Shop requests on page 85

Assigning requestable products to shelf templates

Assign global and special shelf templates to company resources. These company resources are added as product nodes to all the shelves that are created. You can only select those company resources that are labeled with the **IT Shop** option and to which a service item is assigned.

Select one of the tasks in the task view to assign company resources. The tasks are only shown if the **Assignments permitted** and **Direct assignment permitted** options are enabled for the **IT Shop template** role class.

To assign company resources as products to a shelf

1. In the Manager, select the **IT Shop > Shelf templates** category.
2. Select the rule template in the result list.
3. Select the **Assign <company resource>** task.

   In the **Add assignments** pane, assign company resources..

   TIP: In the **Remove assignments** pane, you can remove company assignments.

   To remove an assignment

   - Select the company resource and double-click ✓.
4. Save the changes.

Related topics

- Preparing products for requesting on page 21
- Assigning and removing products on page 54
- Role classes for the IT Shop on page 211

Shelf-filling wizard

Use this task to assign special shelf templates to shops and shopping centers. For more information, see Assigning shelf templates to shops and shopping center templates on page 240.

Assigning shelf templates to shops and shopping center templates

Global shelf templates are immediately distributed to all shops. Assign special shelf templates manually to shops and shopping center templates. You also need to assign shopping center templates to the desired shopping center. This assignment takes place in the shopping center.

To assign a special shelf template to shops and shopping center templates

1. In the Manager, select the **IT Shop > Shelf templates** category.
2. Select a shelf template in the result list.
3. Select **Shelf Filling Wizard**.
4. Select **Create/remove shelves**.
5. In the **Shelf template**, select a special shelf template.
6. Enable the shops and shopping center template to which to assign this shelf template.
7. Click **Apply**.

Table 67: Settings in the shelf filling wizard

Property	Description
Create/remove shelves tab	This shows shops and shopping centers to which shelf templates can be assigned and removed again.
Shelf template	This list displays all available special shelf templates. By default, the shelf template list is preset with the name of shelf template from which the wizard is started.

Property	Description
Filter	This limits the number of shops and shopping center templates displayed. All entries that contain strings that are entered in the filter condition are displayed. Uppercase and lowercase are not taken into account. The filter takes effect after the shelf template has been reselected in the **Shelf templates** list. The filter also affects the view on **Assignment by shopping center templates**.
List of Shops and Shopping Center Templates	• To assign a shelf template, select the check box next to the desired shop or shopping center template. • Use **Assign all** to assign a template to all shops and shopping center templates. • In order to remove the assignments from all shops, click the **Remove all** button. • You can select several entries at one time (**Ctrl + left mouse button** or **Shift + left mouse button**) and change the assignments using the **Invert selection** button. • Click **Apply** to save the changes.
Assignment by shopping center templates tab	Once the DBQueue Processor has calculated the assignments, the shops in which a shelf was created from a shopping center template, are displayed on this tab. This only provides an overview. You cannot edit the assignments. The shops displayed are limited through the filter.

Related topics

- General main data of IT Shop structures on page 219

Deleting shelf templates

If a shelf template is deleted, the **QER | ITShop | Templates | DeleteRecursive** configuration parameter is taken into account. If the configuration parameter is set, you can delete a shelf template without requiring any further steps. When this shelf template is deleted, the shelves and products connected with this template are also deleted from the shops. Pending requests in these shelves are closed; approved requests are canceled. If the parameter is not set, templates cannot be deleted as long as shelves reference it.

To delete shelf templates recursively

1. In the Designer, set the **QER | ITShop | Templates | DeleteRecursive** configuration parameter.
2. In the Manager, select the **IT Shop > Shelf templates** category.

3. Select a shelf template in the result list.
4. Click in the result list.

   The next time the DBQueue Processor runs, the shelves and products connected with this template are also deleted from the shops. Pending requests from these shelves are closed, approved request are canceled.

If the configuration parameter is not set, proceed as follows to delete the shelf template:

To delete a global shelf template

1. In the Manager, select the **IT Shop > Shelf templates** category.
2. Select the global shelf template in the result list.
3. Remove all assigned products.
4. Save the changes.

   All assignments of these products to shelves are removed when the DBQueue Processor runs the next time. Then, the shelf template can be deleted.
5. Click in the result list.

   All shelves based on this template are deleted when the DBQueue Processor runs the next time.

To delete a special shelf template

1. In the Manager, select the **IT Shop > Shelf templates** category.
2. Select the special shelf template in the result list.
3. Remove all assigned products.
4. Save the changes.

   All assignments of these products to shelves are removed when the DBQueue Processor runs the next time.
5. Remove all assignments of the shelf template to shops and shopping center templates.

   All shelves based on this template are deleted when the DBQueue Processor runs the next time.
6. Click in the result list.

To delete a shopping center template

1. In the Manager, select the **IT Shop > Shelf templates** category.
2. Select the shopping center template in the result list.
3. Delete all shopping center assignments.

   All shelves based on this template are deleted when the DBQueue Processor runs the next time.
4. Delete all special shelf template assignments to the shopping center template.
5. Click in the result list.

Detailed information about this topic

- Assigning requestable products to shelf templates on page 239
- Assigning shelf templates to shops and shopping center templates on page 240
- General main data of IT Shop structures on page 219

Custom mail templates for notifications

Mail templates are used to send email messages to requesters and approvers.

For more information about creating and editing mail template, see the *One Identity Manager Operational Guide*.

A mail template consists of general main data such as target format, importance, or mail notification confidentiality, and one or more mail definitions. Mail text is defined in several languages in the mail template. This ensures that the language of the recipient is taken into account when the email is generated.

Related topics

- Notifications in the request process on page 181

Creating and modifying IT Shop mail templates

To create and edit mail templates

1. In the Manager, select the **IT Shop > Basic configuration data > Mail templates** category.

   The result list shows all the mail templates that can be used for IT Shop requests.
2. Select a mail template in the result list and run the **Change main data** task.

   - OR -

   Click in the result list.

   This opens the mail template editor.
3. Edit the mail template.
4. Save the changes.

Detailed information about this topic

- General properties of mail templates on page 244
- Creating and editing mail definitions on page 245

General properties of mail templates

The following general properties are displayed for a mail template.

Table 68: Mail template properties

Property	Meaning
Mail template	Name of the mail template. This name will be used to display the mail templates in the administration tools and in the Web Portal. Translate the given text using the button.
Base object	Mail template base object. A base object only needs to be entered if the mail definition properties of the base object are referenced. Use the `PersonWantsOrg` or `PWOHelperPWO` base object for notifications in the IT Shop.
Report (parameter set)	Report, made available through the mail template.
Description	Mail template description. Translate the given text using the button.
Target format	Format in which to generate email notification. Permitted values are: • **`HTML`**: The email notification is formatted in HTML. Text formats, for example, different fonts, colored fonts, or other text formatting, can be included in HTML format. • **`TXT`**: The email notification is formatted as text. Text format does not support bold, italics, or colored font, or other text formatting. Images displayed directly in the message are not supported.
Design type	Design in which to generate the email notification. Permitted values are: • **`Mail template`**: The generated email notification contains the mail body in accordance with the mail definition. • **`Report`**: The generated email notification contains the report specified under **Report (parameter set)** as its mail body. • **`Mail template, report in attachment`**: The generated email notification contains the mail body in accordance with the mail definition. The report specified under **Report (parameter set)** is attached to the notification as a PDF file.
Importance	Importance for the email notification. Permitted values are **`Low`**, **`Normal`**, and **`High`**.
Confidentiality	Confidentiality for the email notification. Permitted values are **`Normal`**, **`Personal`**, **`Private`**, and **`Confidential`**.
Can unsubscribe	Specifies whether the recipient can unsubscribe email notification. If this option is set, the emails can be unsubscribed through the

Property	Meaning
	Web Portal.
Deactivated	Specifies whether this mail template is disabled.
Mail definition	Selects the mail definition in a specific language. NOTE: If the **Common | MailNotification | DefaultCulture** configuration parameter is set, when the template is opened, the mail definition is loaded and displayed in the email notifications default language.
Language	Language that applies to the mail template. The recipient's language preferences are taken into account when an email notification is generated.
Subject	Subject of the email message.
Mail body	Content of the email message.

Creating and editing mail definitions

Mail texts can be defined in these different languages in a mail template. This ensures that the language of the recipient is taken into account when the email is generated.

NOTE: If the **Common | MailNotification | DefaultCulture** configuration parameter is set, the mail definition is loaded in the default language for email notifications when the template is opened.

To create a new mail definition

1. In the Manager, select the **IT Shop > Basic configuration data > Mail templates** category.

   The result list shows all the mail templates that can be used for IT Shop requests.
2. Select a mail template in the result list and run the **Change main data** task.
3. In the result list, select the language for the mail definition in the **Language** drop-down.

   All active languages are shown. To use another language, in the Designer, enable the corresponding countries. For more information, see the *One Identity Manager Configuration Guide*.
4. Enter the subject in **Subject**.
5. Edit the mail text in the **Mail definition** view with the help of the Mail Text Editor.
6. Save the changes.

To edit an existing mail definition

1. In the Manager, select the **IT Shop > Basic configuration data > Mail templates** category.

   The result list shows all the mail templates that can be used for IT Shop requests.

1. Select a mail template in the result list and run the **Change main data** task.
2. In the **Mail definition** drop-down, select the language for the mail definition.
3. Edit the mail subject line and the body text.
4. Save the changes.

Using base object properties

In the subject line and body text of a mail definition, you can use all properties of the object entered under **Base object**. You can also use the object properties that are referenced by foreign key relation.

To access properties use dollar notation. For more information about using dollar ($) notation, see the *One Identity Manager Configuration Guide*.

Example:

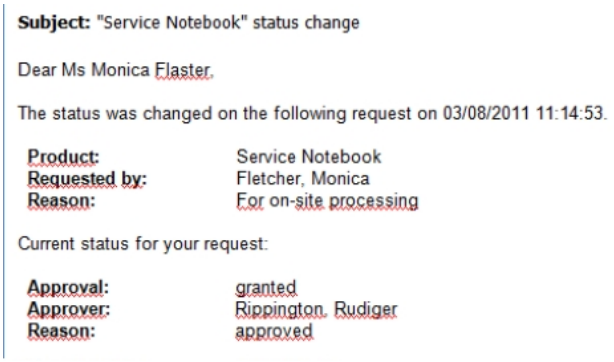
An IT Shop requester should receive email notification about the status of the request.

Table 69: Email notification properties

Property	Value
Base object	PersonWantsOrg
Subject	"$DisplayOrg[D]$" status change
Mail body	Dear $FK(UID_PersonOrdered).Salutation[D]$ $FK(UID_PersonOrdered).FirstName$ $FK(UID_PersonOrdered).LastName$, The status was changed on the following request on $DateHead:Date$. Product: $DisplayOrg[D]$ Requested by: $DisplayPersonInserted$ Reason: $OrderReason$ Current status of your request: Approval: granted

Property	Value
	Approver: $DisplayPersonHead[D]$
	Reason: $ReasonHead[D]$

The generated email notification could look like the following, for example, once it has been formatted.



Subject: "Service Notebook" status change

Dear Ms Monica Flaster,

The status was changed on the following request on 03/08/2011 11:14:53.

Product:	Service Notebook
Requested by:	Fletcher, Monica
Reason:	For on-site processing

Current status for your request:

Approval:	granted
Approver:	Rippington, Rudiger
Reason:	approved

Use of hyperlinks to the Web Portal

You can add hyperlinks to the Web Portal in the mail text of a mail definition. If the recipient clicks on the hyperlink in the email, the Web Portal opens on that web page and further actions can be carried out. In the default version, this method is implemented for IT Shop requests.

Prerequisites for using this method

- The **QER | WebPortal | BaseURL** configuration parameter is enabled and contains the URL to the API Server. You edit the configuration parameter in the Designer.

  `http://<server name>/<application>`

  with:

  `<server name> = name of server`

  `<application> = path to the API Server installation directory`

To add a hyperlink to the Web Portal in the mail text

1. Click the position in the mail text of the mail definition where you want to insert a hyperlink.
2. Open the **Hyperlink** context menu and enter the following information.

- **Display text**: Enter a caption for the hyperlink.
- **Link to**: Select the **File or website** option.
- **Address**: Enter the address of the page in the Web Portal that you want to open.

  NOTE: One Identity Manager provides a number of default functions that you can use to create hyperlinks in the Web Portal.

3. To accept the input, click **OK**.

Default functions for creating hyperlinks

Several default functions are available to help you create hyperlinks. You can use the functions directly when you add a hyperlink in the mail body of a mail definition or in processes

Direct function input

You can reference a function when you add a hyperlink in the **Address** field of the **Hyperlink** context menu.

Syntax

```
$Script(<Function>)$
```

Example:

```
$Script(VI_BuildITShopLink_Show_for_Requester)$
```

Default functions for IT Shop requests

The `VI_BuildITShopLinks` script contains a collection of default functions for composing hyperlinks to directly grant or deny approval of IT Shop requests from email notifications.

Table 70: Functions of the VI_BuildITShopLinks script

Function	Usage
VI_BuildITShopLink_Show_for_Approver	Opens the overview page for request approval in the Web Portal.
VI_BuildITShopLink_Show_for_Requester	Opens the overview page for requests in the Web Portal.
VI_BuildITShopLink_Approve	Approves a request and opens the approvals page in the Web Portal.

Function	Usage
VI_BuildITShopLink_Deny	Denies a request and opens the approvals page in the Web Portal.
VI_BuildITShopLink_AnswerQuestion	Opens the page for answering a question in the Web Portal.
VI_BuildITShopLink_Reject	Opens the page with denied requests in the Web Portal.
VI_BuildAttestationLink_Pending	Opens the page with pending requests in the Web Portal.
VI_BuildITShopLink_Unsubscribe	Creates the link for canceling email notification. This function is used in processes for unsubscribing email notifications.

Customize email signatures

Configure the email signature for mail templates using the following configuration parameters. Edit the configuration parameters in the Designer.

Table 71: Configuration parameters for email signatures

Configuration parameter	Description
Common | MailNotification | Signature	Data for the signature in email automatically generated from mail templates.
Common | MailNotification | Signature | Caption	Signature under the salutation.
Common | MailNotification | Signature | Company	Company name.
Common | MailNotification | Signature | Link	Link to the company's website.
Common | MailNotification | Signature | LinkDisplay	Display text for the link to the company's website.

`VI_GetRichMailSignature` combines the components of an email signature according to the configuration parameters for use in mail templates.

Copying IT Shop mail templates

To copy a mail template

1. In the Manager, select the **IT Shop > Basic configuration data > Mail templates** category.

   The result list shows all the mail templates that can be used for IT Shop requests.
2. Select the mail template that you want to copy in the result list and run the **Change main data** task.
3. Select the **Copy mail template** task.
4. Enter the name of the new mail template in the **Name of copy** field.
5. Click **OK**.

Displaying IT Shop mail template previews

To display a mail template preview

1. In the Manager, select the **IT Shop > Basic configuration data > Mail templates** category.

   The result list shows all the mail templates that can be used for IT Shop requests.
2. Select a mail template in the result list and run the **Change main data** task.
3. Select the **Preview** task.
4. Select the base object.
5. Click **OK**.

Deleting IT Shop mail templates

To delete a mail template

1. In the Manager, select the **IT Shop > Basic configuration data > Mail templates** category.

   The result list shows all the mail templates that can be used for IT Shop requests.
2. Select the template in the result list.
3. Click in the result list.
4. Confirm the security prompt with **Yes**.

Custom notification processes

Set up customized processes to send more email notifications within a request. For more information, see the One Identity Manager Configuration Guide.

You can use following events for generating processes.

Table 72: `PWOHelperPWO` object events

Event	Triggered by
DecisionRequired	Creating a new request.
Remind	Sequence of reminder intervals.

Product bundles

If you want to request products in the Web Portal, select the products you want from a service catalog and place them in the cart. The products remain in the cart until you send the request. You can save all the products in your cart or just individual ones in a product bundle so that you can reuse the products in the cart for future requests. You can add or delete products to product bundles at anytime.

To use a product bundle

- In the Designer, set the **QER | ITShop | ShoppingCartPattern** configuration parameter.

You can create product bundles in the Web Portal and in the Manager. In the following you will learn how to set up product bundles with the Manager. For more information about how to set up product bundles in the Web Portal, see the *One Identity Manager Web Portal User Guide*.

Creating and modifying product bundles

To edit a product bundle

1. In the Manager, select the **IT Shop > Product bundles** category.
2. In the result list, select a product bundle and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the product bundle's main data.
4. Save the changes.

Detailed information about this topic

- General main data of a product bundle on page 252
- Cart items on page 253

General main data of a product bundle

Enter the following properties on the **General** tab.

Table 73: General main data of a product bundle

Property	Description
Product bundle	Name of the product bundle.
Name	Any additional name for the product bundle.
Short name	Short name for the product bundle.
Voucher number	A combination of any characters to uniquely identify the product bundle. If you leave this field empty, One Identity Manager automatically allocates a number when you save.
Owner	Owner of the product bundle. The identity that created the product bundle is automatically entered as the owner. This value can be changed at any time.
Description	Text field for additional explanation.
Public product bundle	Specifies whether the product bundle is available to all One Identity Manager users.
Shared	Specifies whether the product bundle is can be used by all One Identity Manager users. This option can only be changed in the Manager through the user with the **Request & Fulfillment | IT Shop | Administrators** application role. If **Public product bundle** is not set on a shared product bundle, **Shared** is also disabled.

Product bundles can be automatically shared once **Public product bundle** has been set.

To automatically share product bundles

- In the Designer, set the **QER \| ITShop \| ShoppingCartPattern \| AutoQualified** configuration parameter.

Cart items

On the **Cart items** tab, assign products to the product bundle.

To add a new request item to the product bundle

- Click .

  The data fields for entering properties are shown.

Table 74: Cart items

Property	Description
product	Products that can be requested with this product bundle. All service items are shown in the drop-down, whose products are assigned to at least one shelf in the IT Shop. • To add other products to the product bundle, click . • To delete a cart item, click .
Quantity	Number of products to request. You need to customize your Web Portal in order to use these values. For more information about this, see the *One Identity Manager HTML5 Development Guide*.
Additional request data	Additional information is required for the request.

Deleting product bundles

To delete a product bundle

1. In the Manager, select the **IT Shop > Product bundles** category.
2. Select a product bundle in the result list.
3. Click in the result list.

NOTE: Every owner can delete his own product bundles in the Web Portal. One Identity Manager users with the **Request & Fulfillment | IT Shop | Administrators** application role can delete the product bundles of all owners.

Recommendations and tips for transporting IT Shop components with the Database Transporter

For detailed about working with change labels and about transporting changes with the Database Transporter, see the *One Identity Manager Operational Guide*.

To transport IT Shop components with the Database Transporter, take the following into account:

- In one transport package, only include a maximum of one shop with shelves and customer nodes including the dynamic roles and, if necessary, associated approval policies.
- You should not transport products that reference target system entitlements. Target system entitlements are loaded into the database by synchronization and obtain different UIDs in different databases. This means that references to these entitlements do not match up in the products.
- Approval policies, approval workflows, approval steps, and approval procedures should be transported together. If necessary, mail templates and mail definitions must be transported as well.
- If IT Shop components reference application or business roles, they must also be transported along with their child roles.
- Transport translations if required.
- If you want to group several objects and dependencies and other changes into a transport package, work with change labels where possible. In the Database Transporter, you can export change labels to a transport package. You can import the transport package with the Database Transporter.
- Alternatively, you can transport a single object with its dependencies by creating an export in transport format. Then you can import the export with the Database Transporter.

Troubleshooting errors in the IT Shop

Timeout on saving requests

If new requests are saved in bulk in the database a timeout may occur, after importing data, for example.

Probable reason

By default, the approvers responsible are determined during saving. This delays the saving process. No more actions can take place in One Identity Manager until all requests are saved and, therefore, all approvers have been found. Depending on the system configuration, this may cause a timeout to occur when large amounts of data are being processed.

Solution

- In the Designer, disable the **QER | ITShop | DecisionOnInsert** configuration parameter.

Effect

- The requests are saved and a calculation task for determining approvers is queued in the DBQueue. Approvers responsible are determined outside the save process.
- If the requester is also the approver, the approval step is not automatically granted approval. Approvers must explicitly approve their own requests. For more information, see Automatically approving requests on page 144.
- Automatic approval decisions are also met if necessary, but are delayed. This affects requests with self-service, for example.

Bulk delegation errors

You have the option to delegate all your responsibilities to an identity in the Web Portal. If you have a lot of responsibilities, it is possible that not all the delegations are carried out. A delegator can send a notification to themselves if an error occurs.

Probable reason

An error occurred processing delegations. `VI_ITShop_Person Mass Delegate` was stopped, although only a fraction of the delegations has been applied.

Solution

1. Configure the notification procedure.
2. Run all remaining delegations again in the Web Portal.

Related topics

- Bulk delegation notifications on page 191

Process monitoring for requests

For more information about process monitoring in One Identity Manager, see the *One Identity Manager Configuration Guide*.

To configure process monitoring for requests

1. In the Designer, check whether the **Common | ProcessState** configuration parameter is set. If not, set the configuration parameter.

   If this configuration parameter is set, a process monitoring entry (`DialogProcess` table) is created when the request is created.
2. In the Designer, check the **Common | ProcessState | UseGenProcIDFromPWO** configuration parameter.

   If this configuration parameter is set, the GenProcID of an IT Shop request is retained for the entirety of the approval process.

   If the configuration parameter is not set, a new GenProcID is used for each approval decision.
3. In the Designer, check the **QER | ITShop | GenProcIDBehavior** configuration parameter

   Set the configuration parameter and use the value to specify how many GenProcIDs should be generated for a shopping cart's requests.

- **`MultiID`**: Generates a new GenProcID for each shopping cart request.
- **`SingleID`**: Generates one GenProcID for the entire shopping cart. All requests created through the shopping cart are given the same GenProcID.

If the configuration parameter is not set, a separate GenProcID is generated for each shopping cart request.

Appendix A

Configuration parameters for the IT Shop

Additional configuration parameters for the IT Shop are available in One Identity Manager. The following table contains a summary of all applicable configuration parameters for the IT Shop.

Table 75: Overview of configuration parameters

Configuration parameter	Description
QER | ITShop	Preprocessor relevant configuration parameter to control the component parts for the IT Shop. If the parameter is set, the IT Shop components are available. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
QER | ITShop | AutoCloseInactivePerson	This configuration parameter defines whether identities are removed from all customer nodes when they are permanently disabled.
QER | ITShop | AutoDecision	This configuration parameter controls automatic approval of IT Shop requests over several approval levels.
QER | ITShop | AutoPublish	General configuration parameter that defines automatic assignment of system entitlements to the IT Shop.
QER | ITShop | AutoPublish | AADDeniedServicePlan	Preprocessor relevant configuration parameter for automatically adding Microsoft Entra ID service

Configuration parameter	Description
	plans to the IT Shop. If the parameter is set, all service plans are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: Microsoft Entra ID Module
QER | ITShop | AutoPublish | AADDeniedServicePlan | ExcludeList	List of all Microsoft Entra ID service plans that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation.
QER | ITShop | AutoPublish | AADGroup	Preprocessor relevant configuration parameter for automatically adding Microsoft Entra ID groups to the IT Shop. If the parameter is set, all groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: Microsoft Entra ID Module
QER | ITShop | AutoPublish | AADGroup | ExcludeList	List of all Microsoft Entra ID groups that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation. Example: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
QER | ITShop | AutoPublish | AADSubSku	Preprocessor relevant configuration parameter for automatically adding Microsoft Entra ID subscriptions to the IT Shop. If the parameter is set, all subscriptions are automatically assigned as

Configuration parameter	Description
	products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: Microsoft Entra ID Module
QER | ITShop | AutoPublish | AADSubSku | ExcludeList	List of all Microsoft Entra ID subscriptions that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation.
QER | ITShop | AutoPublish | ADSGroup	Preprocessor relevant configuration parameter for automatically adding Active Directory groups to the IT Shop. If the parameter is set, all groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in modules: Active Directory Module, Active Roles Module
QER | ITShop | AutoPublish | ADSGroup | ExcludeList	List of all Active Directory groups that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation. Example: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
QER | ITShop | AutoPublish | ADSGroup | AutoFillDisplayName	The configuration parameter specifies whether the template should be applied to the `ADSGroup.DisplayName` column.
QER | ITShop | AutoPublish |	Preprocessor relevant configuration parameter for

Configuration parameter	Description
O3EDL	automatically adding Exchange Online mail-enabled distribution groups to the IT Shop. If the parameter is set, all distribution groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: Exchange Online Module
QER | ITShop | AutoPublish | O3EDL | ExcludeList	List of all Exchange Online mail-enabled distribution groups that must not to be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation. Example: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
QER | ITShop | AutoPublish | O3EUnifiedGroup	Preprocessor relevant configuration parameter for automatically adding Microsoft 365 groups to the IT Shop. If the parameter is set, all groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: Exchange Online Module
QER | ITShop | AutoPublish | O3EUnifiedGroup | ExcludeList	List of all Microsoft 365 groups that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation.
QER | ITShop | AutoPublish | O3TTeam	Preprocessor relevant configuration parameter for automatically adding Microsoft Teams teams to the IT Shop. If the parameter is set, all teams are

Configuration parameter	Description
	automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: Microsoft Teams Module
QER | ITShop | AutoPublish | O3TTeam | ExcludeList	List of all Microsoft Teams teams that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation.
QER | ITShop | AutoPublish | PAGUsrGroup	Preprocessor relevant configuration parameter for automatically adding PAM user groups to the IT Shop. If the parameter is set, all user groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: Privileged Account Governance Module
QER | ITShop | AutoPublish | PAGUsrGroup | ExcludeList	List of all PAM user groups that are not to be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation. Example: `.*Administrator.*|.*Admins|.*Operators`
QER | ITShop | AutoPublish | SPSGroup	Preprocessor relevant configuration parameter for automatically adding SharePoint groups to the IT Shop. If the parameter is set, all groups are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled.

Configuration parameter	Description
	If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: SharePoint Module
QER | ITShop | AutoPublish | SPSGroup | ExcludeList	List of all SharePoint groups that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation. Example: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
QER | ITShop | AutoPublish | OLGRole	Preprocessor relevant configuration parameter for automatically adding OneLogin roles to the IT Shop. If the parameter is set, all roles are automatically assigned as products to the IT Shop. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: OneLogin
QER | ITShop | AutoPublish | OLGRole| ExcludeList	List of all OneLogin roles that must not be automatically assigned to the IT Shop. Each entry is part of a regular search pattern and supports regular expression notation. Example: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
QER | ITShop | ChallengeRoleRemoval	General configuration parameter for dealing with role assignments that are modified by data import. Removal of role memberships can be challenged with the help of temporary requests.
QER | ITShop |	This configuration parameter contains the validity

Configuration parameter	Description
ChallengeRoleRemoval | DaysOfValidity	period (in days) of temporary requests for challenged role memberships.
QER | ITShop | ChallengeRoleRemoval | Department	Temporary requests of department memberships are supported.
QER | ITShop | ChallengeRoleRemoval | Department | Primary	Temporary membership of the previous department is requested if changes are made to the primary membership in departments.
QER | ITShop | ChallengeRoleRemoval | ITShopOrg	This configuration parameter contains the product node that is assigned to the requested assignment resource.
QER | ITShop | ChallengeRoleRemoval | Locality	Temporary requests of location memberships are supported.
QER | ITShop | ChallengeRoleRemoval | Locality | Primary	Temporary membership of the previous location is requested if changes are made to the primary membership in locations.
QER | ITShop | ChallengeRoleRemoval | Org	Temporary requests of business role memberships are supported.
QER | ITShop | ChallengeRoleRemoval | Org | Primary	Temporary membership of the previous business role is requested if changes are made to the primary membership in business roles.
QER | ITShop | ChallengeRoleRemoval | ProfitCenter	Temporary requests of cost center memberships are supported.
QER | ITShop | ChallengeRoleRemoval | ProfitCenter | Primary	Temporary membership of the previous cost center is requested if changes are made to the primary membership in cost centers.
QER | ITShop | DecisionOnInsert	This configuration parameter controls approval of a request the moment is it added.

QER | ITShop | DefaultSenderAddress	Sender's default email address for sending automatically generated notifications about requests. Replace the default address with a valid email address.
	Syntax:
	`sender@company.com`
	Example:
	`noreply@company.com`

Configuration parameter	Description
	You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (<>). Example: `One Identity <noreply@company.com>`
QER | ITShop | Delegation	Preprocessor relevant configuration parameter for controlling model components for delegation and role membership. Changes to the parameter require recompiling the database. If the parameter is set, delegation components are available. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
QER | ITShop | DeleteClosed	This configuration parameter specifies whether closed requests are deleted.
QER | ITShop | DeleteClosed | Aborted	This configuration parameter specifies the maximum retention time (in days) of canceled requests.
QER | ITShop | DeleteClosed | Dismissed	This configuration parameter specifies the maximum retention time (in days) of denied requests.
QER | ITShop | DeleteClosed | Unsubscribed	This configuration parameter specifies the maximum retention time (in days) of canceled requests.
QER | ITShop | ExceededValidUntilUnsubscribe	The configuration parameter specifies whether requests of limited validity are unsubscribed or canceled once their limit is exceeded. If the parameter is set and the request has the status **`Assigned`** or **`Renewal`**, the request is unsubscribed if not other request exist for the product that is currently in effect. Expired requests with the status **`Unsubscription`** and **`Unsubscribed`** are no longer taken into account. Expired requests with the status **`approved, pending, request`** are canceled. If the parameter is not set, the request will be canceled in any case.
QER | ITShop | GapBehavior	Defines behavior when checking the validity period of new requests.
QER | ITShop | GapBehavior |	This configuration parameter specifies which

Configuration parameter	Description
GapDefinition	requests are checked.
QER | ITShop | GapBehavior | GapFitting	This configuration parameter specifies whether validity periods of two or more pending requests can overlap.
QER | ITShop | GenProcIDBehavior	This configuration parameter specifies how many GenProcIDs should be generated for a shopping cart's requests. If the configuration parameter is not set, a separate GenProcID is generated for each shopping cart request.
QER | ITShop | LimitOfNodeCheck	Maximum number of product nodes that can be generated or deleted by a DBQueue Processor run. Once this number is exceeded, a task for generating the rest of the nodes is queued in the DBQueue.
QER | ITShop | MailApproval | Account	Name of the user account for authenticating the mailbox used for approval by mail.
QER | ITShop | MailApproval | AppID	Exchange Online application ID for authentication with OAuth 2.0. If the value is not set, the **Basic** or the **NTML** authentication method is used.
QER | ITShop | MailApproval | DeleteMode	Specifies the way emails are deleted from the inbox.
QER | ITShop | MailApproval | Domain	Domain of the user account for authenticating the mailbox used for approval by mail.
QER | ITShop | MailApproval | ExchangeURI	URL of the Microsoft Exchange web service for accessing the mailbox. If this is not given, `AutoDiscover` mode is used to detect the URL.
QER | ITShop | MailApproval | Inbox	Microsoft Exchange mailbox to which approvals by mail are sent.
QER | ITShop | MailApproval | Password	Password of the user account for authenticating the mailbox used for approval by mail.
QER | ITShop | MailTemplateIdents | AnswerToApprover	This mail template is used to send a notification with an answer to a question from an approver.
QER | ITShop | MailTemplateIdents | InformAddingPerson	This mail template is used to notify approvers that an approval decision has been made for the step they added.
QER | ITShop | MailTemplateIdents | InformDelegatingPerson	This mail template is used to notify approvers that an approval decision has been made for the step they delegated.

Configuration parameter	Description
QER | ITShop | MailTemplateIdents | ITShopApproval	Mail template used for requests made through "Approval by mail".
QER | ITShop | MailTemplateIdents | QueryFromApprover	This mail template is used to send a notification with a question from an approver to an identity.
QER | ITShop | MailTemplateIdents | RequestApproverByCollection	This mail template is used for generating an email when there are pending requests for an approver. If this configuration parameter is not set, a "Mail template request" or "Mail template reminder" for single approval steps can be entered to send an email for each request. If this configuration parameter is set, single mails are not sent.
QER | ITShop | OnWorkflowAssign	This configuration parameter specifies how pending orders are handled when an approval, change, or cancellation workflow is reassigned to the approval policy.
QER | ITShop | OnWorkflowUpdate	This configuration parameter specifies how pending orders are handled when the approval workflow is changed.
QER | ITShop | PeerGroupAnalysis	This configuration parameter allows automatic approval of requests by peer group analysis.
QER | ITShop | PeerGroupAnalysis | ApprovalThreshold	This configuration parameter defines a threshold for peer group analysis between 0 and 1. The default value is 0.9.
QER | ITShop | PeerGroupAnalysis | CheckCrossfunctionalAssignment	This configuration parameter specifies whether functional areas should be take into account in peer group analysis. If the parameter is set, the request is only approved if the request's recipient and the requested product belong to the same functional area.
QER | ITShop | PeerGroupAnalysis | IncludeManager	This configuration parameter specifies whether identities can be added to the peer group who have the same manager as the request's recipient.
QER | ITShop | PeerGroupAnalysis | IncludePrimaryDepartment	This configuration parameter determines whether identities that are primary members of the primary department of the request's recipient are included in the peer group.
QER | ITShop | PeerGroupAnalysis | IncludeSecondaryDepartment	This configuration parameter determines whether identities that are a secondary members of the

Configuration parameter	Description
	primary or secondary department of the request's recipient are included in the peer group.
QER | ITShop | PersonInsertedNoDecide	This configuration parameter specifies whether the identity that triggered the request may approve it.
QER | ITShop | PersonOrderedNoDecide	This configuration parameter specifies whether the identity for whom the request was triggered, may approve it.
QER | ITShop | PersonInsertedNoDecideCompliance	This configuration parameter specifies whether the identity that initiated the request can issue exception if compliance rules are violated by the request.
QER | ITShop | PersonOrderedNoDecideCompliance	This configuration parameter specifies whether the identity for whom the request was initiated can issue exception if compliance rules are violated by the request.
QER | ITShop | Recommendation	Threshold values for approval recommendations are defined under this configuration parameter.
QER | ITShop | Recommendation | ApprovalRateThreshold	This configuration parameter specifies the threshold for the approval rate. The approval rate determines the proportion of approvals for this product in previous requests that were decided with the same approval procedure. The lower the threshold, the more likely granting approval will be recommended.
QER | ITShop | Recommendation | PeerGroupThreshold	This configuration parameter specifies the threshold for the peer group factor. The peer group factor determines the proportion of identities in the peer group who already own the product. The lower the threshold, the more likely granting approval will be recommended.
QER | ITShop | Recommendation | RiskIndexThreshold	This configuration parameter specifies the threshold for the risk index of the request's recipient. The current request is already taken into account. The higher the threshold, the more likely granting approval will be recommended.
QER | ITShop | ReducedApproverCalculation	This configuration parameter specifies, which approval steps are recalculated if the IT Shop approver must be recalculated.
QER | ITShop | ReplaceAssign-mentRequestOnLeaveCU	If an identity leaves a customer node, all assigned requests are canceled and assignment requests are converted to direct assignments. If this parameter is

Configuration parameter	Description
	set, then assignment requests can be transferred to the manager or central approver group, and to the UID_PersonFallback if necessary. (Note: These identities must have approval authorization for this assignment).
QER | ITShop | ReplaceAssignmentRequestOnLeaveCU | UID_PersonFallback	UID_Person is an identity that is set as the fallback if no other request recipient can be found for an assignment request. This identity must be a customer in all shops in which assignments can be requested.
QER | ITShop | ReuseDecision	This configuration parameter specifies if approval granted by one approver to all approval steps of an approval process is transferred. If the parameter is set, the current step is approved if an approval step is reached in the approval process for which an identity with approval authorization has already granted approval. If the parameter is not set, the approver must separately approve each step for which they have approval authorization. If approval has not been granted, it is not transferred.
QER | ITShop | ShoppingCartPattern	This configuration parameter specifies whether product bundles can be used in the IT Shop.
QER | ITShop | ShoppingCartPattern | AutoQualified	This configuration parameter specifies whether public product bundles are automatically labeled as "shared" or whether they have to be manually shared by a manager.
QER | ITShop | ShowClosedAssignmentOrders	This configuration parameter specifies whether the manager of an organization or business role can view completed assignment requests for their organization or business role. If this parameter is not set, the manager can only view open assignment requests for their organization or business role.
QER | ITShop | Templates	Preprocessor relevant configuration parameter for controlling the database model components for the Shelf Filling Wizard. Changes to the parameter require recompiling the database. Shelf templates can be used. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and

Configuration parameter	Description
	triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
QER | ITShop | Templates | DeleteRecursive	This configuration parameter specifies whether the recursive deletion is allowed from shelf templates. This configuration parameter is disabled by default.
QER | ComplianceCheck | DisableSelfExceptionGranting	Excludes rule violators from becoming exception approvers. If this parameter is set, no one can approve their own rule violations.
QER | ComplianceCheck | EnableITSettingsForRule	IT Shop properties for the compliance rule are visible and can be edited.
QER | Person | Starling	Specifies whether connecting to the One Identity Starling cloud platform is supported. Initiate your subscription within your One Identity on-prem product and join your on-prem solutions to our One Identity Starling cloud platform. Giving your organization immediate access to a number of cloud-delivered microservices, which expand the capabilities of your One Identity on-prem solutions. We will continuously make available new products and features to One Identity Starling. For a free trial of our One Identity Starling offerings and to get the latest product feature updates, visit cloud.oneidentity.com.
QER | Person | Starling | ApiEndpoint	Token endpoint for logging in to One Identity Starling The value is determined by the Starling configuration wizard.
QER | Person | Starling | ApiKey	Authentication credentials for logging in to One Identity Starling The value is determined by the Starling configuration wizard.
QER | Person | Starling | UseApprovalAnywhere	This configuration parameter defines whether requests and attestation cases can be approved by adaptive cards.
QER | Person | Starling | UseApprovalAnywhere | SecondsToExpire	This configuration parameter specifies the time in seconds by which the adaptive card must be answered.
QER | WebPortal	General configuration parameter for Web Portal settings.

Configuration parameter	Description
QER | WebPortal | BaseURL	API Server URL. This address is used in mail templates to add hyperlinks to the Web Portal.
QER | WebPortal | DisplayName	This configuration parameter contains the display name of the Web Portal. This name is used in mail templates.
QER | WebPortal | PasswordResetURL	URL of the API Server that deploys the Password Reset Portal. This web address is used for navigation.
QER | WebPortal | PersonChangeWorkdesk	This configuration parameter specifies whether Web Portal users can change their default workdesk. If the configuration parameter is set, users can relocate their workdesk through the Web Portal.
QER | WebPortal | ShowProductImages	This configuration parameter specifies whether pictures of products are displayed in the Web Portal.
Hardware | Workdesk | WorkdeskAutoPerson	If this configuration parameter is set, creating a workdesk automatically creates an associated identity. This identity can be used to make requests for this workstation.

Some general configuration parameters are also relevant for the IT Shop.

Table 76: Additional configuration parameters

Configuration parameter	Description
Common | MailNotification | Signature	Data for the signature in email automatically generated from mail templates.
Common | MailNotification | Signature | Caption	Signature under the salutation.
Common | MailNotification | Signature | Company	Company name.
Common | MailNotification | Signature | Link	Link to the company's website.
Common | MailNotification | Signature | LinkDisplay	Display text for the link to the company's website.

Configuration parameter	Description
Common | ProcessState	If this configuration parameter is set, a process monitoring entry (`DialogProcess` table) is created when the request is created.
Common | ProcessState | PropertyLog	When this configuration parameter is set, changes to individual values are logged and shown in the process view. Changes to the parameter require recompiling the database. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
Common | ProcessState | UseGenProcIDFromPWO	If this configuration parameter is set, the GenProcID of an IT Shop request is retained for the entirety of the approval process. If the configuration parameter is not set, a new GenProcID is used for each approval decision.
TargetSystem | ADS | ARS_SSM	Preprocessor relevant configuration parameter for controlling the database model components for Active Roles Self-Service Management in the One Identity Manager IT Shop. If the parameter is set, Self-Service Management components are available. Changes to this parameter require the database to be recompiled. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*. In effect in module: Active Roles Module

Appendix B

Request statuses

The following table gives an overview of all statuses a request can have.

Table 77: Request statuses

Status (technical name)	Description
New (`New`)	A product was requested. The request was added in the database.
Request (`OrderProduct`)	The request is currently in the approval process. An approval decision has not yet been reached.
Approved (`Granted`)	The approval process is complete. The request is granted approval.
Pending (`Waiting`)	The request is granted approval. A valid from date was given in the request. This date has not been reached yet.
Assigned (`Assigned`)	The request was granted approval and assigned.
Renewal (`OrderProlongate`)	The request with limited validity was assigned. A renewal has been applied for and is in the approval process. An approval decision has not yet been reached.
Unsubscription (`OrderUnsubscribe`)	This product was canceled. The cancellation is currently in the approval process. An approval decision has not yet been reached.
Unsubscribed (`Unsubscribed`)	The approval process is complete. The cancellation was granted approval.
Denied (`Dismissed`)	The approval process is complete. The request was denied.
Canceled (`Aborted`)	The request was canceled by a user or for technical reasons.

Table 78: Status summary

Pending requests	Requests with the status request, renewal, canceled.
Approved requests	Requests with the status approved, pending, assigned, renewal, canceled.
Assigned requests	Requests with the status assigned, renewal, canceled.
Closed requests	Requested with the status unsubscribed, denied, canceled.

Appendix C

Examples of request results

Request results differ depending on whether a simple or multiple request resource or an assignment is requested. The following figures illustrate the differences.

Figure 12: Request for a single request resource

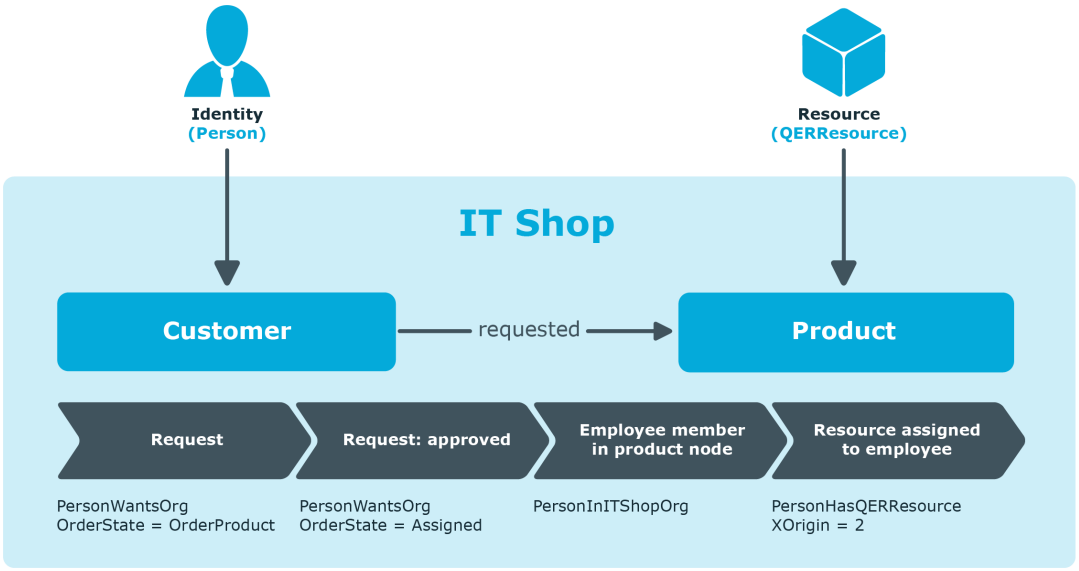


Figure 13: Request for a multi-request resource

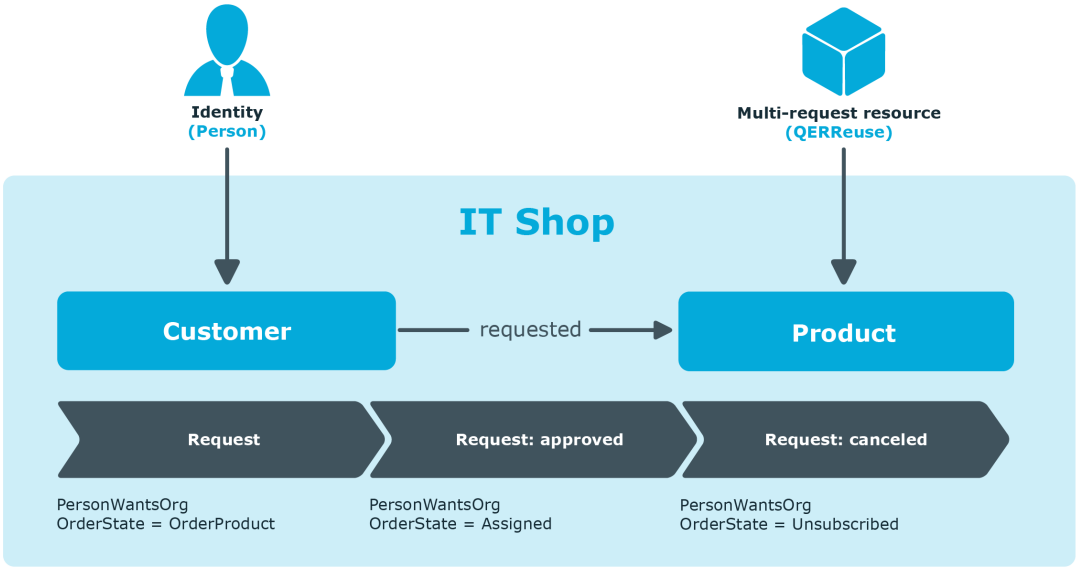


Figure 14: Request for a requestable/unsubscribable resource

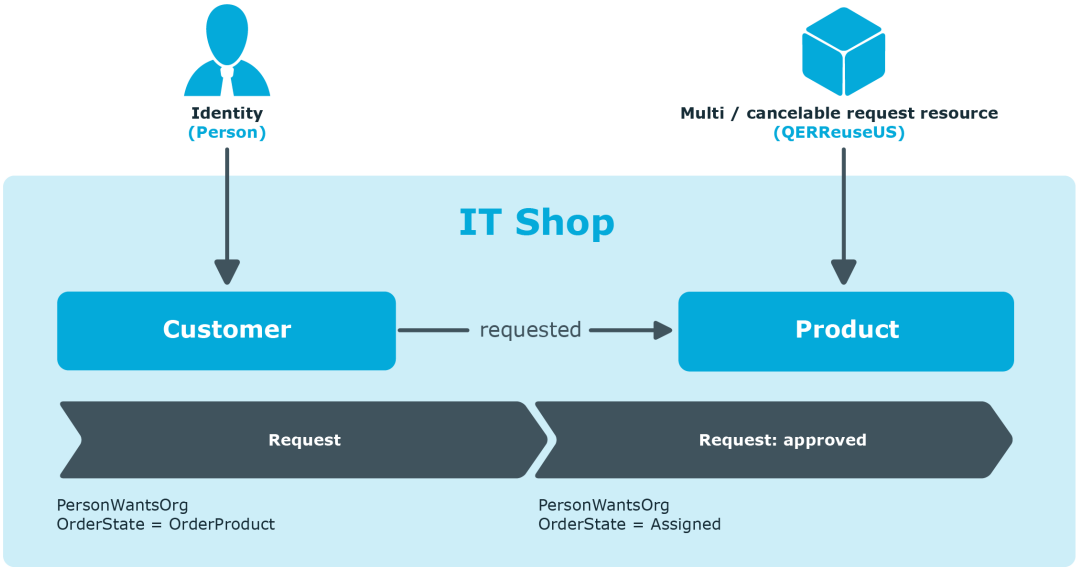


Figure 15: Request for a department membership

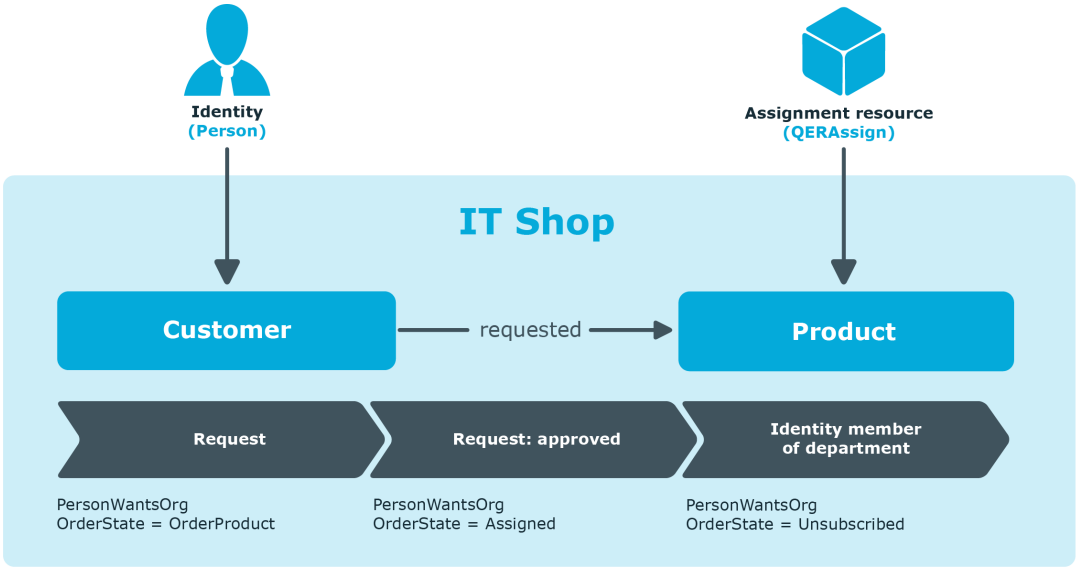
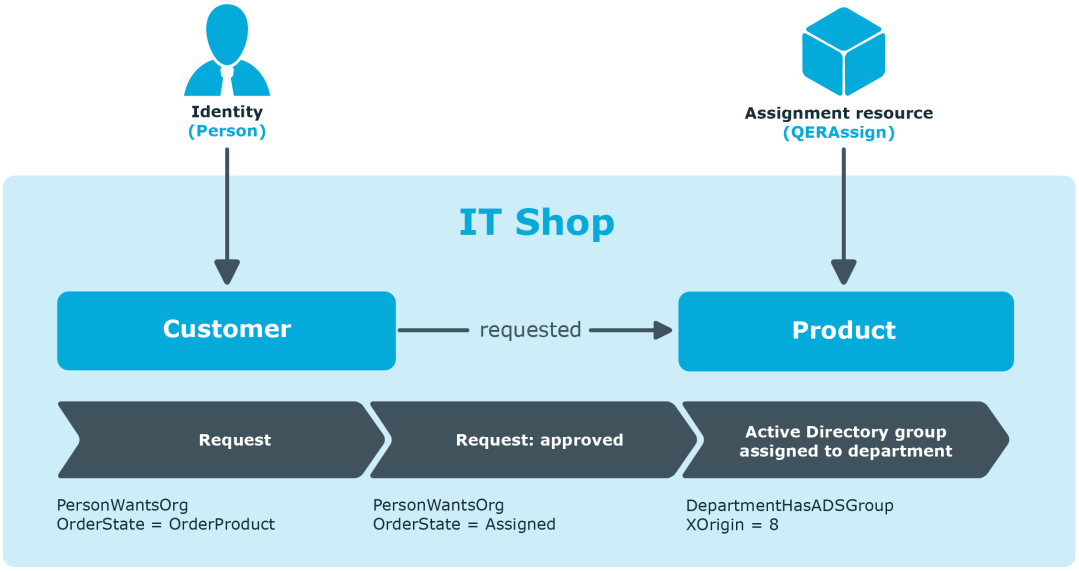


Figure 16: Request for assignment of an Active Directory group to a department



Appendix D

Example of defining request properties

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

adaptive card 195-196
- apply 198
- approver 197
- channel 197
- create 198, 202
- deactivate 201-202
- delete 198
- edit 198
- evaluate 202
- language 201
- process QER_PWOHelpterPWO approve anywhere 198
- request template 200
- script 202
- template 198, 201

administrator 12
Application Governance Module 16
application role
- administrator 12
- attestors 217
- chief approval team 130, 215
- clean up 83
- delete 83
- delete obsolete product owner 83
- product owners 12, 216

approval 101
approval level
- connect 101
- edit 94

approval policies
- approval workflow 86
- assign 222, 238
- cancellation workflow 86
- copy 89
- create 85
- determine 103
- effective 103
- mail template 86
- overview form 90
- priority 86
- renewal workflow 86
- role type 86
- verify 88

approval procedure 95, 105
- Active Directory group product owner and additional owner 110
- add 125
- additional owner of the Active Directory group 111
- application entitlement approver 115
- application owner 111
- approvals made externally 119, 123
- attestor assigned service item 116
- back to recipient 118
- back to requester 118
- calculated approval 119, 122
- compliance check (simple) 134
- compliance check (simplified) 119
- condition 126
- copy 129
- custom 125
- delete 130

escalation 155
exception approver for worst rule violation 136
exception approvers for violated rules 116
identity in additional request data 118
manager of cost center given in the request 109
manager of department given in the request 109
manager of recipient's cost center 108
manager of recipient's department 108
manager of shelf's cost center 109
manager of shelf's department: 109
manager of shopping center's cost center 109
manager of shopping center's department 109
manager of shop's cost center 109
manager of shop's department 109
Manager of the requested role 109
members of a certain role 110
owner of the object in any request parameter of the request properties 111-112
owner of the requested privileged access request 111
product owners 110
query 126
recipient's manager 108
role approvers (IT) of recipient's department 115
role approvers (IT) of recipient's primary cost center 115
role approvers (IT) of recipient's primary location 115
role approvers (IT) of the cost center given in the request 114
role approvers (IT) of the department given in the request 114
role approvers (IT) of the recipient's primary business role 115
role approvers of the cost center given in the request 114
role approvers of the department given in the request 113
role approvers of the recipient's primary business role 114
role approvers of the recipient's primary cost center 115
role approvers of the recipient's primary department 114
role approvers of the recipient's primary location 114
self-service 119-120
shelf owner 110
shop owner 110
shopping center owner 110
specific role Manager 109
target system manager of the requested system entitlement 117
violation rule exception approver 136
waiting for further approval 120
approval process 85, 87, 103
approval rate
request 150
approval reason 209
approval recommendation for approvers 149
configure 152
criteria 150
approval step
approval procedure 95
edit 95

escalation 155
mail template 95
relevance for compliance 95
reminder interval 95
rule check 95
timeout behavior 95
timeout interval 95
approval workflow
copy 101
delete 102
overview form 102
renewal 104
set up 90
system halt 93
timeout interval 93
unsubscribe 105
approver
adaptive card 195-197
approval by email 191
approving own request 142
channel 197
notification 182, 184, 188-189
recalculate 130
restrictions 142
select 105
assignment rate
request 150
assignment request 60
approver 64
convert to direct assignment 66
grant approval 64
obtain 68
prepare 60
remove recipient from customer node 66
service item 60
unsubscribe 65
assignment resource 60
add 64
assign shelf 70
for a business role 62
for an application role 63
overview form 70
remove from shelf 70
resource type 68
risk index 68
service item 68

B

business partner 212
business role
assign service item 30

C

cancellation workflow 105, 174, 181
cart item 253
change of manager 178
chief approval team 130, 215
comparison value 132
connector
on approval 101
on escalation 101
on rejection 101
on reroute 101
cost center
assign service item 30
create product nodes 56
cross-functional product 147-148, 150
currency 26

customer
delete 228
dynamic assignments 226
relocate 49, 66, 176
customer node
assign identities directly 225
delete 228
delete identities 66
new 224
overview form 227
set up 223

D

decision
by peer group 147-148
with recommendation 149
default approval policy 87
default approval workflow 103
default assignment resources 69
default mail template 191
default service category 38
default service item 27
delayed decision 120
delegation
approval notification 185
deputize 71
error 191
grant approval 74
notification 189, 191
prepare 73
service item 72
single delegation 71
deny 101
department
assign service item 30
dynamic role
customer node 226

E

email notification
set up 181
escalation 101
exception approver 136
approving own request 139
limit 139
on self-service 142
expiry date 172-174, 184
extended property
assign service item 31

F

fallback approver 157
functional area 214
assign service item 31

G

GenProcID 256
going live with an IT Shop 14

I

identity
assign to customer node 225
transform existing assignment in request 76
Identity Lifecycle 14
IT Shop
approval process 85
edit 206

IT Shop structure 218

L

location
assign service item 30

M

mail template
approval policies 86
approval step 95
base object 244, 246
confidentiality 244
design type 244
edit 243
hyperlink 247
importance 244
language 245
mail definition 245
report 244
target format 244
unsubscribe 244
manufacturer 212
Multi-factor authentication 59

N

notification
approval 185, 189
default mail template 191
delegation 189
deny 185, 189
deny approval 188
escalation 187
expiry 184
mail template 181
on delegation 185
product change 190
query 188
quit 187
recipient 181
refuse approval 188
reject approval 188
reminder 182
renewal 190
request 182, 188
sender 181
unsubscribe 190

P

peer group analysis
configure for request 148
for request 147
peer group factor
request 150
price 26
processing status 208
product 16
assign 56, 222
assign to template 239
change 32, 58
cross-functional 147-148
dependent 27
move 57, 230-231
multi requestable 19
not available 50
prepare 21
relocate 49, 57, 176, 231
remove 57
replace 32, 58
report 34

service item 21-22
terms of use 50
unsubscribe 181
validity period 48
product bundle 251
administrator 252
cart item 253
create 251
delete 253
product 253
public product bundle 252
share 252
product owners 12, 81
clean up 83
delete 83
delete unused application role 83

R

reason 209
renewal
approver 104
renewal workflow 104, 173
request
approval by mail 191
approval by Starling Cloud Assistant 195-196
approval history 170
approval recommendation 149
approval sequence 169
approve automatically 144, 159
approved 273
assigned 273
assignment request 60
unsubscribe 65
by approver 142
cancel 180, 204
change approval workflow 176
close pending 176
closed 205, 273
copy existing assignment 75
delete 205
details 169
escalate 155
expiry date 172-174, 184
extend 173
for employees 178
monitor 256
multi-request 171
new manager 178
notification 181, 184
open 273
overview 169
query 154
quit 57, 160, 231
reject approval 176
relocate 176
role 60, 203
sequence 167
status 273
timeout 155, 159-160
unsubscribe 174, 181
validity period 172, 174
withdraw 180
request parameter 40
settings 41
request procedure
archiving 205
record 205
request property
copy 47

log 40
main data 41
request recipient
accept terms of use 163
notification 190
request status 273
reroute 101
resource
multi requestable 19
risk assessment 132
functional area 214
risk factor
request 150
risk index 68, 132
role
request membership automatically 203
transform existing assignment in request 80
role classes 211
role type 212, 219, 237
rule check 133
compliance check (simple) 134
find exception approver 136
on self-service 142

S

service catalog 27, 36, 38
service category
approval policies 36
attestors 36
log 36
process information 36
product owners 36
request property 36
service item
approval policies 23
assign business role 30
assign cost center 30
assign department 30
assign extended properties 31
assign function area 31
assign hierarchical role 29
assign location 30
assign tag 33
attestors 23
cost center 23
enter tag 52
image 27
log 22
manufacturer 23
multi-request 23
open site 32
overview form 34
overview of all assignments 35
parent 29
product description 32
product owners 23
reason type 23
relocate 23, 49
replace 32
report 34
request property 23
risk assessment 29
subordinate 29
terms of use 50
validity 23
validity period 48
shelf
administrator 219

approval policies 222, 238
assign product 222
attestors 219
cost center 219
delete 228
department 219
deputy 219
location 219
move 230-231
overview form 223
role type 219
set up 219
shelf filling wizard 240
shelf template
administrator 237
assign 219, 240
assign product 239
attestors 237
cost center 237
create 236-237
delete 241
delete shelf 228
department 237
deputy 237
global 232, 236
location 237
role type 237
special 232, 236
shop
administrator 219
approval policies 222
attestors 219
cost center 219
delete 229
department 219
deputy 219
location 219
move 230-231
overview form 223
set up 219
shopping center
administrator 219
approval policies 222
attestors 219
cost center 219
delete 230
department 219
deputy 219
location 219
overview form 223
set up 219
shelf template 219
shopping center template 232
assign 240
create 236
delete 241
single delegation 73
standard reason 209
usage type 210
Starling Cloud Assistant
approver 197
channel 197
status
request 273
system entitlement
add to IT Shop (automatic) 81

T

tag 52
assign service item 33, 53

create 33
overview form 54
template
product bundle 251
shelf template 232
terms of use 50
accept 163
overview form 52
PDF file 51

U

unsubscribe
approver 105
user account
transform existing assignment in request 77

V

valid from date 172
valid until date 172
validity period
verify 174

W

workdesk
transform existing assignment in request 78
Workflow Editor 90