



One Identity Manager 9.1.1

Identity Management Base Module Administration Guide

Copyright 2023 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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


Patents

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

Trademarks

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

Legend

-  **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

One Identity Manager Identity Management Base Module Administration Guide
Updated - 28 March 2023, 21:46

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

Contents

Basics for mapping company structures in One Identity Manager	10
Hierarchical role structure basic principles	11
Inheritance directions within a hierarchy	11
Discontinuing inheritance	13
Basic principles for assigning company resources	15
Direct company resource assignments	16
Indirect company resource assignments	16
Secondary assignment	16
Primary assignment	17
Assigning company resources through dynamic roles	19
Assigning company resources through IT Shop requests	19
Basics of calculating inheritance	20
Calculating inheritance by hierarchical roles	21
Calculation of assignments	22
Preparing hierarchical roles for company resource assignments	24
Possible assignments of company resources through roles	25
Permitting assignments of employees, devices, workdesks, and company resources to roles	29
Blocking inheritance using roles	30
Preventing employees, devices, or workdesks from inheriting individual roles	31
Preventing inheritance to individual employees, devices, or workdesks	31
Inheritance exclusion: Specifying conflicting roles	33
Dynamic roles	35
Creating and editing dynamic roles	36
Tips about conditions for dynamic roles	37
Testing dynamic role conditions	38
Calculating role memberships for dynamic roles	39
Schedules for calculating dynamic roles	40
Creating and editing dynamic role schedules	40
Starting dynamic role schedules immediately	43
Assigning dynamic roles to schedules	43

Calculating dynamic roles immediately if objects change	44
Editing properties for immediate recalculation	46
Calculating role memberships for dynamic roles immediately	47
Excluding dynamic roles from recalculation	47
Excluding employees from dynamic roles	48
Removing employees from the exclusion list	48
Main data of exclude lists for dynamic roles	49
Displaying the dynamic role overview	49
Main data for dynamic roles	50
Departments, cost centers, and locations	52
One Identity Manager users for managing departments, cost centers, and locations ...	53
Basic information for departments, cost centers, and locations	55
Role classes for departments, cost centers, and locations	56
Assigning role types to role classes for departments, cost centers, and locations ..	57
Role types for departments, cost centers, and locations	57
Creating role types for departments, cost centers, and locations	58
Assigning role classes to role types for departments, cost centers, and locations ..	59
Functional areas for departments, cost centers, and locations	59
Attestors for departments, cost centers, and locations	61
Approvers and approvers (IT) for departments, cost centers, and locations	62
Creating and editing departments	63
General main data for departments	63
Contact data for departments	66
Functional area and risk assessment for departments	66
Creating and editing cost centers	67
General main data for cost centers	68
Functional area and risk assessment for cost centers	70
Creating and editing locations	71
General main data for locations	72
Location address information	74
Configuring location networks	75
Directions to location	75
Functional area and risk assessment for locations	75
Setting up IT operating data for departments, cost centers, and locations	76
Modify IT operating data	80

Assigning employees, devices, and workdesks to departments, cost centers, and locations	81
Assigning company resources to departments, cost centers, and locations	82
Creating dynamic roles for departments, cost centers, and locations	85
Dynamic roles with incorrectly excluded employees	86
Assign organizations	86
Specifying inheritance exclusion for departments, cost centers, and locations	87
Assigning extended properties to departments, cost centers, and locations	89
Certifying departments, cost centers, and locations	90
Reports about departments, cost centers, and locations	91
Employee administration	92
One Identity Manager users for employee administration	93
Basic data for employee main data	94
Creating and editing business partners for external employees	95
Mail templates for notifications about employees	96
Creating and editing mail definitions for employees	97
Base object for mail templates about employees	98
Editing mail templates for employees	98
Employee's central user account	99
Employee's default email address	100
Employee's central password	101
Mapping multiple employee identities	102
Employee identity types	103
Password policies for employees	105
Predefined password policies	105
Applying employee password policies	106
Changing the password policy for password columns	107
Assigning password policies to departments, cost centers, locations, and business roles	107
Editing password policies for employees	108
Creating password policies for employees	109
General main data for password policies	109
Password policy settings	110
Character classes for passwords	111
Custom scripts for password requirements	113

Checking passwords with a script	113
Generating passwords with a script	115
Defining the excluded list for passwords	116
Checking employee passwords	116
Generating passwords for testing employees	117
Informing employees about expiring passwords	117
Displaying locked employees and system users	118
Creating and editing employees	118
General employee main data	119
Organizational employee main data	122
Address data for employees	124
Miscellaneous employee main data	125
Disabling and deleting employees	128
Temporarily deactivating employees	128
Permanently deactivating employees	129
Reactivate permanently deactivated employees	130
Deferred deletion of employees	130
Deleting all employee related data	131
Limited access to One Identity Manager	131
Changing the certification status of employees	132
Assigning company resources to employees	133
Assigning employees to departments, cost centers, and locations	138
Assigning employees to business roles	139
Adding employees to IT Shop custom nodes	139
Assigning application roles to employees	140
Assigning resources directly to employees	141
Assigning software directly to employees	141
Assigning system roles directly to employees	142
Assigning subscribable reports directly to employees	142
Displaying the origin of employees' roles and entitlements	143
Analyzing role memberships and employee assignments	145
Displaying the employees overview	146
Displaying and deleting employees' Webauthn security keys	147
Determining the language for employees	148
Determining employees working hours	149

Manually assigning user accounts to employees	150
Entering calls for employees	150
Assigning extended properties to employees	150
Employee reports	151
Managing devices and workdesks	154
Basic data for device admin	155
Creating and editing device models	155
General main data for device models	156
Inventory data for device models	157
Creating and editing business partners	158
Creating and editing device statuses	159
Creating and editing workdesk statuses	160
Creating and editing workdesk types	160
Creating and editing devices	161
General main data for devices	163
Device networking data	165
Assigning company resources to devices	167
Assigning devices to departments, cost centers, and locations	168
Assigning devices to business roles	169
Displaying the device overview	170
Entering service agreements and calls for devices	170
Creating and editing workdesks	171
General main data of workdesks	171
Location information for workdesks	173
Additional information for workdesks	173
Assigning company resources to workdesks	174
Assigning workdesks to departments, cost centers, and locations	176
Assigning workdesks to business roles	177
Assigning software directly to workdesks	178
Assigning system roles directly to workdesks	178
Displaying the workdesk overview	179
Assigning devices to workdesks	179
Assigning workdesks to employees	180
Entering calls for workdesks	181
Asset data for devices	181

Creating and editing asset classes for devices	182
Creating and editing asset types for devices	182
Entering investments and investment plans for devices	183
Editing device asset data	183
Main data for devices' asset data	184
Commercial data for devices	185
Managing resources	187
One Identity Manager users for managing resources	188
Basic data for resources	189
Resource types	189
Creating and editing resources	190
Main data for resources	190
Assigning resources to employees	192
Assigning resources to departments, cost centers, and locations	192
Assigning resources to business roles	193
Assigning resources directly to employees	193
Adding resources to the IT Shop	194
Adding resources in system roles	195
Displaying the resources overview	195
Assigning extended properties to resources	196
Creating and editing multi-request resources	196
Main data for multi-request resources	197
Assigning multi-request resources to employees	198
Adding multi-request resources to the IT Shop	199
Displaying the multi-request resource overview	200
Reports about resources	201
Setting up extended properties	202
One Identity Manager users for managing extended properties	202
Creating property groups for extended properties	203
Creating and editing extended properties	204
Main data for extended properties	204
Assigning extended properties to property groups	205
Assigning additional property groups to extended properties	206
Specifying scope limits for extended properties	206

Displaying the extended properties overview	207
Assigning objects to extended properties	208
Appendix: Configuration parameters for managing departments, cost centers, and locations	209
Appendix: Configuration parameters for managing employees	211
Appendix: Configuration parameters for managing devices and workdesks	214
About us	216
Contacting us	216
Technical support resources	216
Index	217

Basics for mapping company structures in One Identity Manager

One Identity Manager supplies employees in a company with company resources. For example, permissions, or software, according to their function. To do this, the company structures are represented in hierarchical role form in One Identity Manager.

Roles are objects through which company resources can be assigned. Employees, devices, and workdesks are assigned to roles as members. Members can obtain their company resources through these roles when One Identity Manager is appropriately configured.

Company resource assignments are not made to individual employees, devices, or workdesks but centrally and then inherited automatically through a predefined distribution list.

In One Identity Manager, the following roles are defined for mapping company structures:

- Departments, cost centers, and locations
Departments, cost centers, locations, and business roles are each mapped to their own hierarchy under **Organizations**. This is due to their special significance for daily work schedules in many companies.
- Business roles
Business roles map company structures with similar functionality that exist in addition to departments, cost centers, and locations. This might be projects groups, for example. For more information about business roles, see the *One Identity Manager Business Roles Administration Guide*.
| NOTE: This function is only available if the Business Roles Module is installed.
- Application roles
Application roles are used to grant One Identity Manager object permissions to One Identity Manager users. For more information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Detailed information about this topic

- [Hierarchical role structure basic principles](#) on page 11
- [Basic principles for assigning company resources](#) on page 15

- [Basics of calculating inheritance](#) on page 20
- [Preparing hierarchical roles for company resource assignments](#) on page 24

Hierarchical role structure basic principles

Departments, cost centers, locations, and application roles are arranged hierarchically. Assigned company resources are inherited by members through these hierarchies. Company resource assignments are not made to individual employees, devices or workdesks but centrally and then inherited automatically through a predefined distribution list.

Hierarchies can either be created following the top-down or the bottom-up model in One Identity Manager. In the top-down model, roles are defined based on the area of activity and the company resources required to fulfill the activities are assigned to the roles. In the case of the bottom-up model, company resource assignments are analyzed and the roles result from this.

Detailed information about this topic

- [Inheritance directions within a hierarchy](#) on page 11
- [Discontinuing inheritance](#) on page 13

Inheritance directions within a hierarchy

The direction of inheritance decides the distribution of company resources within a hierarchy. One Identity Manager basically recognizes two directions of inheritance:

- Top-down inheritance

In One Identity Manager, top-down inheritance maps the default structure within a company. With its help, a company's multilevel form can be represented with main departments and respective subdepartments.

- Bottom-up inheritance

Whereas in top-down inheritance, assignments are inherited in the direction of more detailed classifications, bottom-up inheritance operates in the other direction. This inheritance direction was introduced to map project groups in particular. The aim being, to provide someone coordinating several project groups with the company resources in use by each of the project groups.

NOTE: The direction of inheritance is only taken into account in relation to the inheritance of company resources. The direction of inheritance does not have any effect on the selection of the manager responsible. The manager with a parent role is always

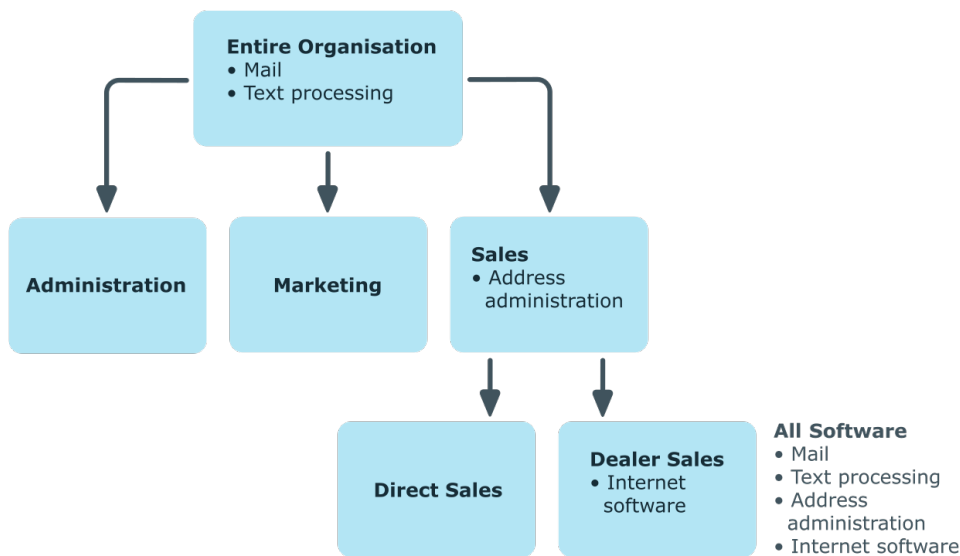
responsible for all child roles.

The effect on the allocation of company resources is explained in the following example for assigning an application.

Example: Assigning company resources top-down

In the diagram above a section of a company's structure is illustrated. In addition, software applications are listed that are assigned to the respective department. An employee in dealer sales is assigned all the software applications that are allocated to their department and all those on the entire organization path. In this case, they are email, text processing, address management and internet software.

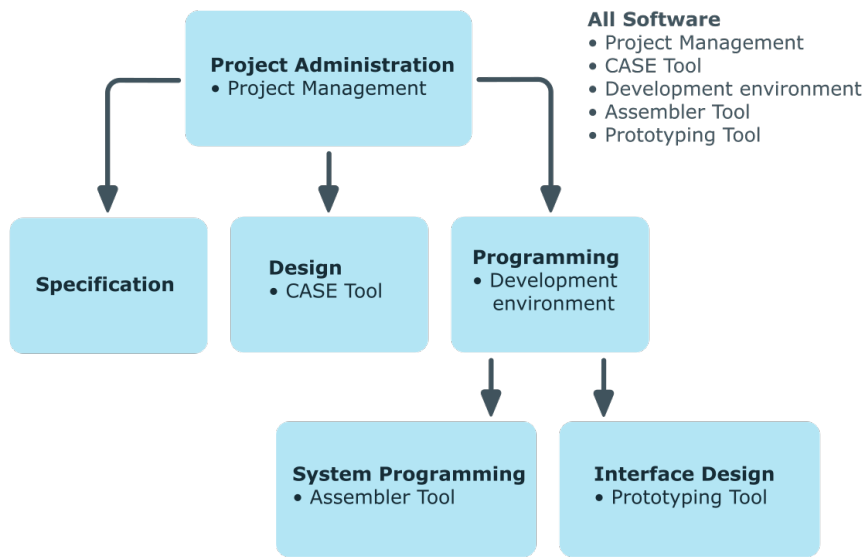
Figure 1: Assignment through top-down inheritance



Example: Assigning company resources bottom-up

The next figure shows bottom-up inheritance based on a project framework. In addition, software applications are listed that are assigned to the respective project group. An employee from the "Project lead" project group receives software applications from the project group as well as those from the projects groups below. In this case, it is project management, CASE tool, development environment, assembler tool, and prototyping tool.

Figure 2: Assignment through bottom-up inheritance



Discontinuing inheritance

There are particular cases where you may not want to have inheritance over several hierarchical levels. That is why it is possible to discontinue inheritance within a hierarchy. The point at which the inheritance should be discontinued within a hierarchy is specified by the **Block inheritance** option. The effects of this depend on the chosen direction of inheritance.

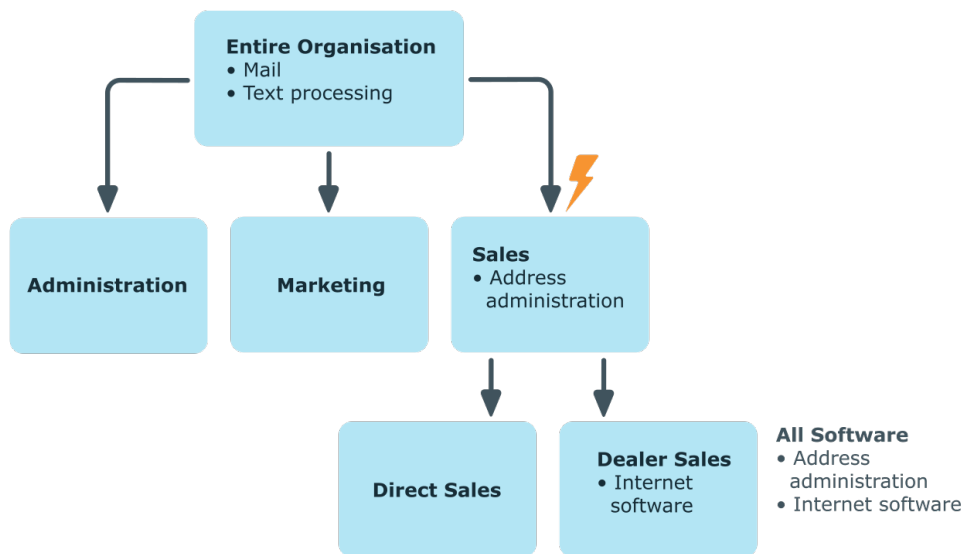
- Roles marked with the **Block inheritance** option do not inherit any assignments from parent levels in top-down inheritance. It can, however, pass on its own directly assigned company resources to lower level structures.
- In bottom-up inheritance, the role labeled with the “Block inheritance” option inherits all assignments from lower levels in the hierarchy. However, it does not pass any assignments further up the hierarchy.

The **Block inheritance** option does not have any effect on the calculation of the manager responsible.

Example: Discontinuing inheritance top-down

If the **Block inheritance** option is set for the "Sales" department in the top-down example, it results in sales employees only being assigned the "Address management" software and employees in the "Dealer sales" department inherit the "Address management" and "Internet" software. Software applications in the "Entire organization" department are however, assigned to employees in the "Sales" and "Dealer sales" departments.

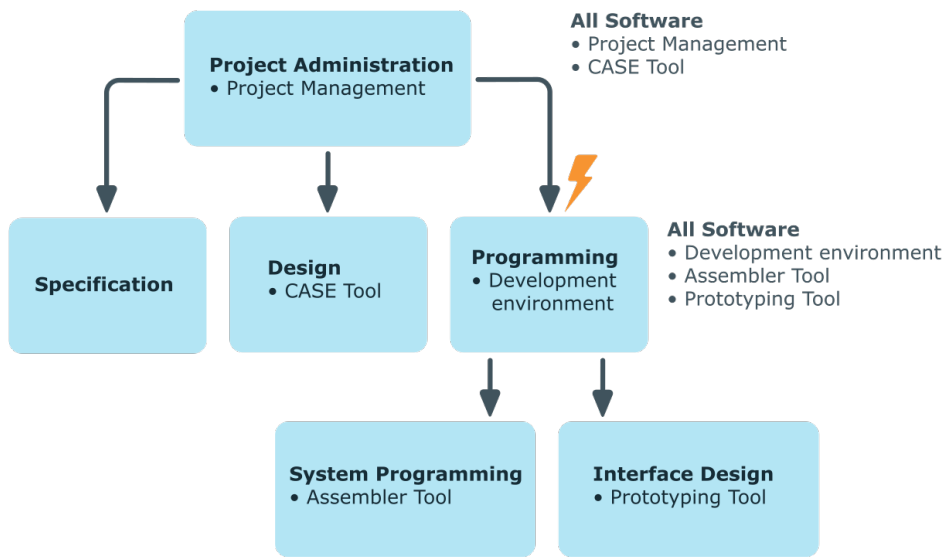
Figure 3: Discontinuing inheritance top-down



Example: Discontinuing inheritance bottom-up

An employee from the "Programming" project group receives software applications from the project group as well as those from the projects groups below. In this case, the development environment, assembler tool and the prototyping tool. If the "Programming" project group has labeled with the **Block inheritance** option, it no longer passes down inheritance. As a result, only the CASE tool is assigned to employees in the "Project lead" project group along with the software application project management. Software applications from the "Programming", "System programming", and "Interface design" projects groups are not distributed to the project lead.

Figure 4: Discontinuing inheritance bottom-up



Related topics

- [Blocking inheritance using roles](#) on page 30

Basic principles for assigning company resources

You can assign company resources to employees, devices, and workdesks in the One Identity Manager. You can use different assignments types to assign company resources.

Assignments types are:

- [Direct company resource assignments](#)
- [Indirect company resource assignments](#)
- [Assigning company resources through dynamic roles](#)
- [Assigning company resources through IT Shop requests](#)

Direct company resource assignments

Direct assignment of company resources results from the assignment of a company resource to an employee, device, or workdesk, for example. Direct assignment of company resources makes it easier to react to special requirements.

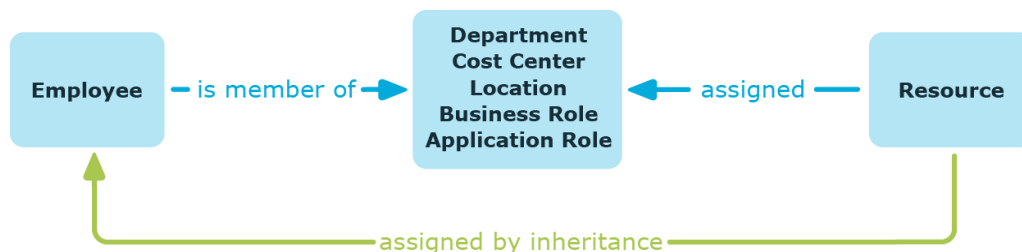
Figure 5: Schema of a direct assignment based on the example of an employee



Indirect company resource assignments

In the case of indirect assignment of company resources, employees, devices, and workdesks are arranged in departments, cost centers, locations, business roles, or application roles. The total of assigned company resources for an employee, device, or workdesk is calculated from the position within the hierarchies, the direction of inheritance (top-down or bottom-up) and the company resources assigned to these roles. In the Indirect assignment methods a difference between primary and secondary assignment is taken into account.

Figure 6: Schema of an indirect assignment based on the employee example



Related topics

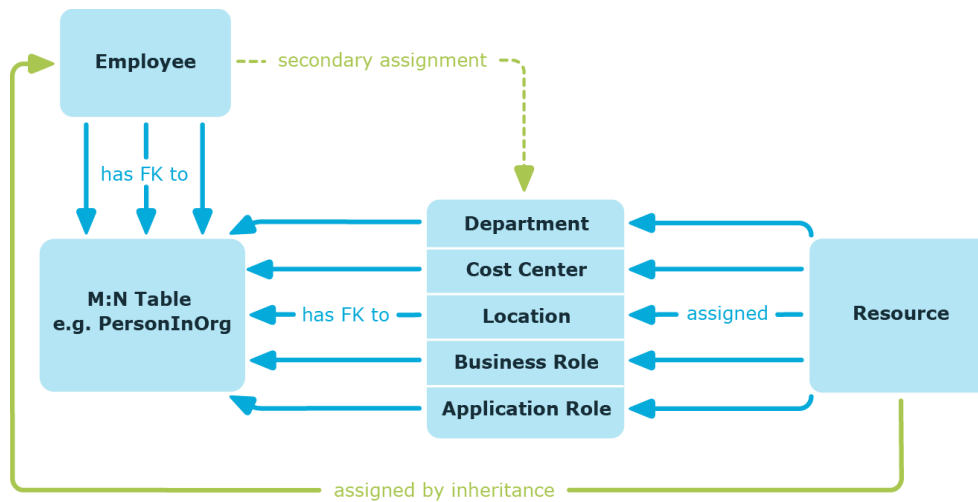
- [Secondary assignment](#) on page 16
- [Primary assignment](#) on page 17

Secondary assignment

You make a secondary assignment by classifying an employee, a device, or a workdesk within a role hierarchy. Secondary assignment is the default method for assigning and inheriting company resources through roles. In the role classes for departments, locations,

cost centers, business roles, and application roles, specify whether a secondary assignment of company resources to employees, device, and workdesk is possible.

Figure 7: Secondary assignment inheritance schema



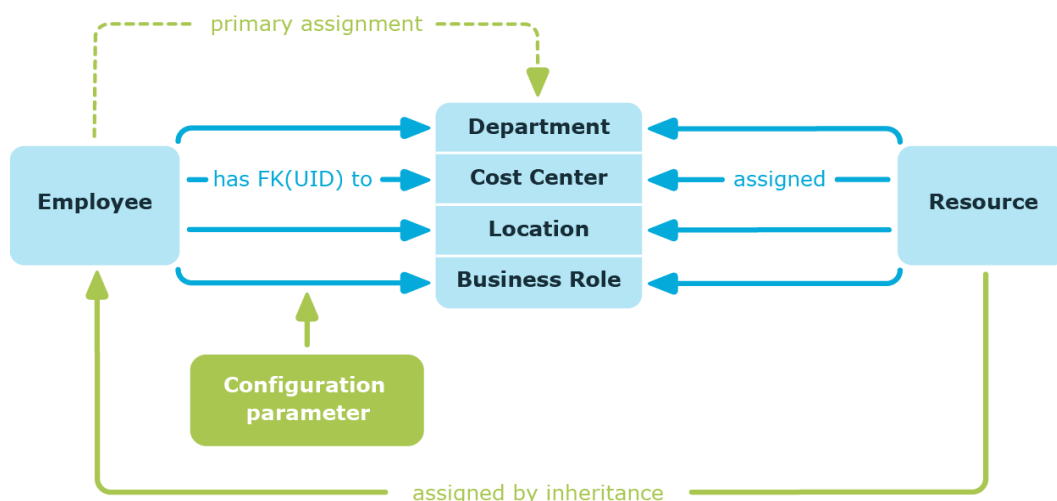
Related topics

- [Permitting assignments of employees, devices, workdesks, and company resources to roles on page 29](#)

Primary assignment

You make a primary assignment using a department, cost center, or location foreign key reference in employee, device and workdesk objects. To do this, use the role fields on the employee, device, and workdesk main data forms. Primary assignment inheritance can be enabled through configuration parameters. Primary assignment is enabled by default for employee objects.

Figure 8: A primary assignment schema



NOTE: Changes to the configuration parameter result in the inheritance data being recalculated! That means: if the primary assignment is disabled at a later date, the inheritance data created in this way will be removed from the database.

Table 1: Configuration parameters for primary assignment

Configuration parameter	Effect when set
QER Structures Inherit Employee	Employees can inherit through primary assignments.
QER Structures Inherit Employee GroupExclusion	Employees inherit assignments from their primary department (Person.UID_Department).
QER Structures Inherit Employee FromLocality	Employees inherit assignments from their primary location (Person.UID_Locality).
QER Structures Inherit Employee FromProfitCenter	Employees inherit assignments from their primary cost center (Person.UID_ProfitCenter).
QER Structures Inherit Hardware	Devices can inherit through primary assignments.
QER Structures Inherit Hardware FromDepartment	Devices inherit assignments from their primary department (Hardware.UID_Department).
QER Structures Inherit Hardware FromLocality	Devices inherit assignments from their primary location (Hardware.UID_Locality).
QER Structures Inherit Hardware FromProfitCenter	Devices inherit assignments from their primary cost center (Hardware.UID_ProfitCenter).
QER Structures Inherit Workdesk	Workdesks can inherit through primary assignment.
QER Structures Inherit	Workdesks inherit assignments from their primary

Configuration parameter	Effect when set
Workdesk FromDepartment	department (Workdesk.UID_Department).
QER Structures Inherit Workdesk FromLocality	Workdesks inherit assignments from their primary location (Workdesk.UID_Locality).
QER Structures Inherit Workdesk FromProfitCenter	Workdesks inherit assignments from their primary cost center (Workdesk.UID_ProfitCenter).

Assigning company resources through dynamic roles

Assignment through dynamic roles is a special case of indirect assignment. Dynamic roles are used to specify role memberships dynamically. Employees, devices, and workdesks are not permanently assigned to a role, just when they fulfill certain conditions. A check is performed regularly to assess which employees, devices, or workdesks fulfill these conditions. This means the role memberships change dynamically. For example, company resources can be assigned dynamically to all employees in a department in this way; if an employee leaves the department they immediately lose the resources assigned to them.

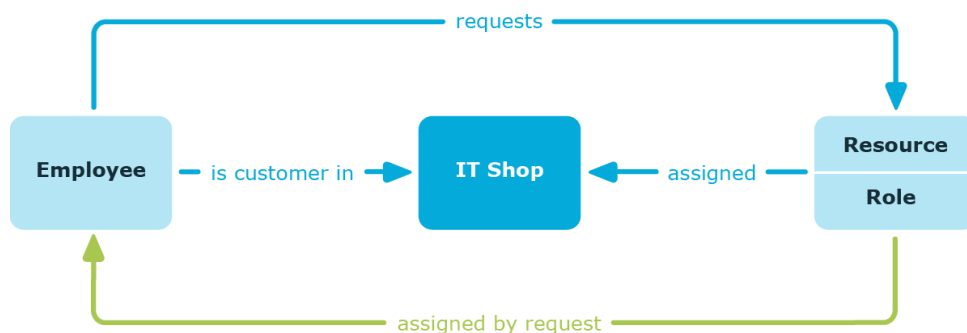
Related topics

- [Dynamic roles](#) on page 35

Assigning company resources through IT Shop requests

Assignment through the IT Shop is a special case of indirect assignment. Add employees to a shop as customers so that company resources can be assigned through IT Shop requests. All company resources assigned as product to this shop can be requested by the customers. Requested company resources are assigned to the employees after approval is granted. Role memberships can be requested through the IT Shop as well as company resources.

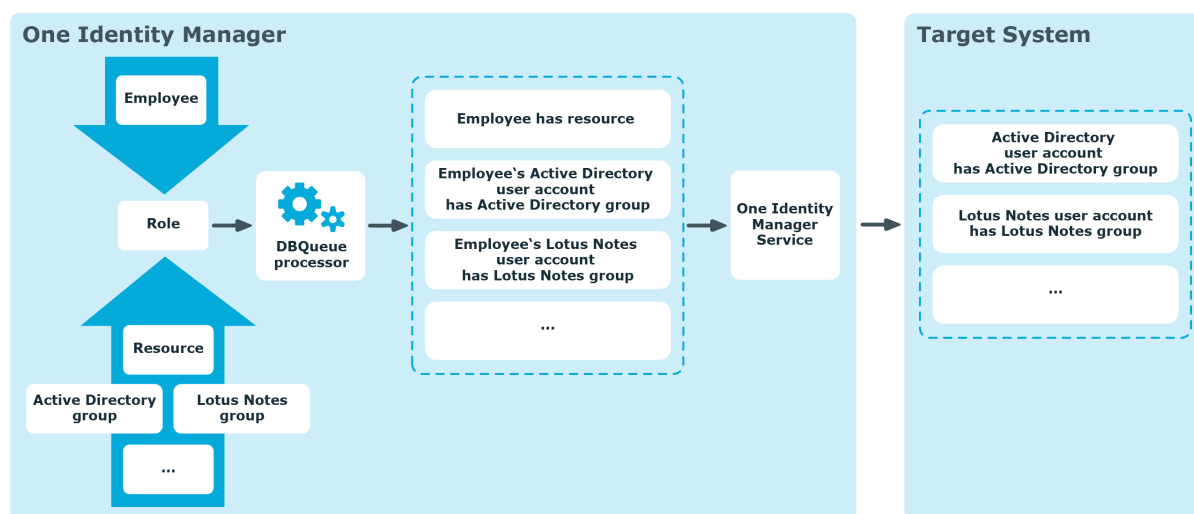
Figure 9: Schema of assignment by requests



Basics of calculating inheritance

Objects assigned through inheritance are calculated by the DBQueue Processor. Tasks are added to the DBQueue when assignments relevant to inheritance are made. These tasks are processed by the DBQueue Processor and result in follow-on tasks for the DBQueue or in processes for process component `HandleObjectComponent` in the Job queue. Resulting assignments of permissions to user accounts in the target system are inserted, modified, or deleted during process handling.

Figure 10: Overview of inheritance calculation



Detailed information about this topic

- [Calculating inheritance by hierarchical roles](#) on page 21
- [Calculation of assignments](#) on page 22

Calculating inheritance by hierarchical roles

Employees, devices, and workdesks can only be members in roles that are extensions of the BaseTree table. These role are display in views, each of which represents a certain of the BaseTree table. To map company structures, the One Identity Manager data model obtains the following views:

Table 2: BaseTree table views

View	Meaning
Department	Graphical representation of departments
Locality	Graphical representation of locations
PROFITCENTER	Graphical representation of cost centers
ORG	Graphical representation of business roles
AERole	Application role mapping

NOTE: Because the views are subsets of the BaseTree table, all the inheritance mechanisms described below also apply to the views.

Inheritance comes from the BaseTree table. The BaseTree table can map any number of hierarchical role structures using the UID_Org - UID_ParentOrg relationship. These are stored in the BaseTreeCollection table. All the roles inherited from the given role are listed and, depending on their subset of the table BaseTree there is a corresponding, so-called *Collection table containing a subset of the role hierarchy.

The following relations apply in the BaseTreeCollection table:

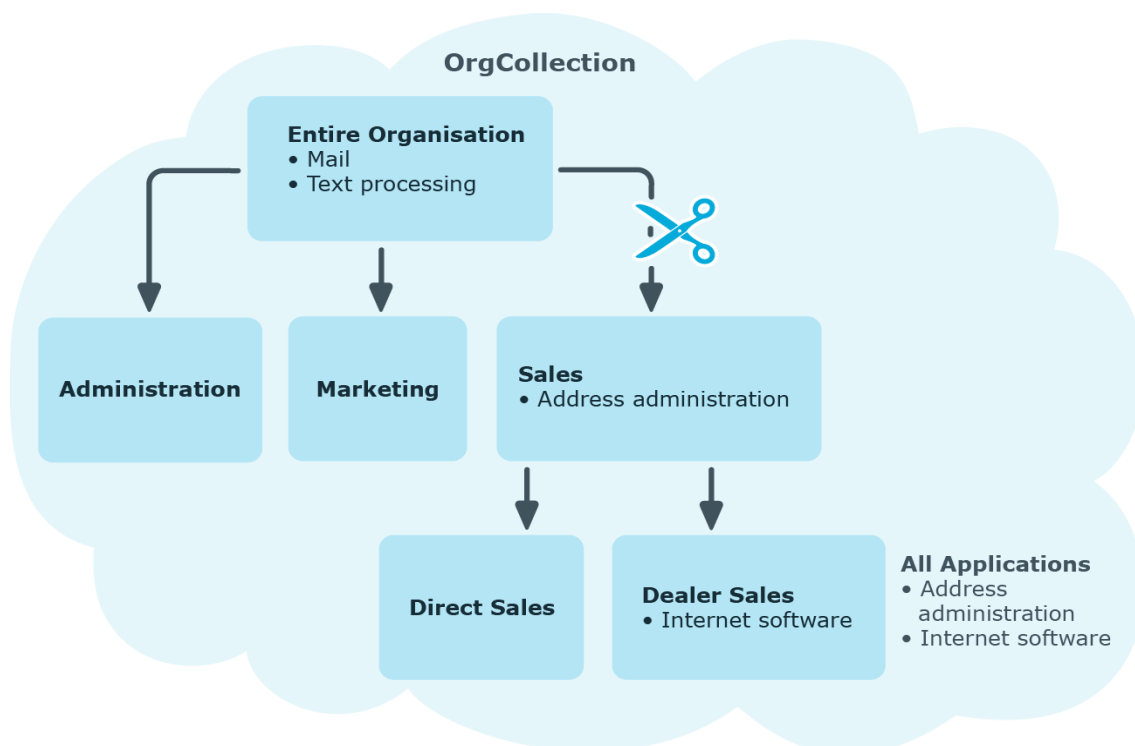
- UID_Org is the role that inherits.
- UID_ParentOrg is the role that passes down inheritance.

This principle also applies to bottom-up trees that pass inheritance from bottom to top, even if the parent relationship from the BaseTree table appears to be reversed.

Each role inherits from itself.

Each role in a role hierarchy must be related to the OrgRoot table (Role classes). OrgRoot is the anchor for role hierarchies. A role hierarchy is always mapped for one role class only. Roles from different role classes may not be in one and the same role hierarchical or point to each other through a parent-child relationship.

Figure 11: Hierarchical role structure based on an OrgCollection



A role inherits everything that is assigned to its parents in the role hierarchy including those it assigned to itself. If the number of roles from which the role has inherited something changes, the assigned objects are recalculated for all members of this role. If the number of assigned objects of one class changes, the objects assigned in this class are recalculated for all members of the role. If a software application is assigned to a parent role, the members of the BaseTreeHasApp table are recalculated.

The members of a role inherit all their assignments through primary and secondary role structures in accordance with the BaseTree table and also previous structures in accordance with the BaseTreeCollection table .

Calculation of assignments

When inheritance is calculated, an entry is made for each assignment in the corresponding assignment table. Each table, in which assignments are mapped, has an X0origin column. The origin of an assignment is stored in this column as a bit field. Each time an entry is made in the assignment table, the bit position is changed according to the assignment type. Each assignment type changes only its allocated bit position.

That means:

- Bit 0: direct assignment.
- Bit 1: indirect assignment but not through a dynamic role.

- Bit 2: assignment through a dynamic role.
- Bit 3: assignment through an assignment request.
- Bit 4: module specific bit. For more information, see the administration guide of the module in which the bit is used.

Table 3: Possible values for column XOrigin

Bit 3	Bit 2	Bit 1	Bit 0	Value in XOrigin	Meaning
0	0	0	1	1	Only directly assigned.
0	0	1	0	2	Only indirectly assigned.
0	0	1	1	3	Directly and indirectly assigned.
0	1	0	0	4	Assigned through dynamic roles.
0	1	0	1	5	Assigned directly and through dynamic roles.
0	1	1	0	6	Assigned indirectly and through dynamic roles.
0	1	1	1	7	Assigned directly, indirectly, and through dynamic roles.
1	0	0	0	8	Assignment request.
1	0	0	1	9	Assigned by assignment request and directly.
1	0	1	0	10	Assigned by assignment request and indirectly.
1	0	1	1	11	Assigned by assignment request, directly, and indirectly.
1	1	0	0	12	Assigned by assignment request and through dynamic roles.
1	1	0	1	13	Assigned by assignment request, directly, and through dynamic roles.
1	1	1	0	14	Assigned by assignment request, indirectly, and through dynamic roles.
1	1	1	1	15	Assignment request, direct, indirect, and through dynamic roles.

Special features of inheriting assignments through a role hierarchy

NOTE: If an assignment is inherited through a role hierarchy, **bit 1** is set on the inherited assignment. Inherited assignments are consequently, always assigned indirectly even if they were originally created directly through dynamic role or an assignment request.

Example:

An Active Directory group assignment was requested for the "Europe" location. The "Madrid" sub-location inherits this assignment. In the LocalityHasADSGroup table, XOrigin is set as follows:

- Location "Europe": XOrigin='8' (assignment resource)
- Location "Madrid": XOrigin='2' (indirect assignment)

Effectiveness of assignments

The XIsInEffect column shows whether an assignment is in effect. For example, if an employee is deactivated, marked for deletion, or classified as a security risk, inheritance of company resources can be prohibited for this employee. The group assignment is maintained but the assignment has no effect.

DBQueue Processor monitors changes to the XOrigin column. The XIsInEffect column is recalculated when changes are made to the value in XOrigin.

Preparing hierarchical roles for company resource assignments

One Identity Manager supplies a configuration, which support immediate usage of hierarchical roles for departments, cost centers, locations, and application roles. However, it may be necessary to make additional role assignments depending on the company structure.

You should check the following settings and make adjustments as required:

- Specify whether employees, devices, and workdesks and company resources may be assigned to roles.

Employee, device, workdesk, and company resource assignments are predefined for departments, cost centers, location, and application roles. The configuration of application role assignments cannot be changed.

- Define the direction of inheritance with the hierarchy.

Top down inheritance is defined for departments, cost centers, locations, and application roles.

- Limit inheritance for specific roles if necessary.

You can specify whether inheritance of company resources can be limited for single employees, devices, or workdesks.

- If required, define roles that are mutually exclusive.

By specifying conflicting roles, you can prevent employees, devices, or workdesks being added to roles which contain mutually excluding company resources.

Detailed information about this topic

- [Possible assignments of company resources through roles](#) on page 25
- [Permitting assignments of employees, devices, workdesks, and company resources to roles](#) on page 29
- [Blocking inheritance using roles](#) on page 30
- [Preventing employees, devices, or workdesks from inheriting individual roles](#) on page 31
- [Preventing inheritance to individual employees, devices, or workdesks](#) on page 31
- [Inheritance exclusion: Specifying conflicting roles](#) on page 33

Possible assignments of company resources through roles

Employees, devices, and workdesks can inherit company resources through indirect assignment. To do this, employees, devices, and workdesks may be members of as many roles as required. Employees, devices, and workdesks obtain the necessary company resources through defined rules.

To assign company resources to roles, apply the appropriate tasks to the roles.

The following table shows the possible assignments of company resources to employees, workdesks, and devices using roles.

NOTE: Company resources are defined in the One Identity Manager modules and are not available until the modules are installed.

Table 4: Possible assignments of company resources through roles

Assignable Company Resource	Members in Roles	
	Employees	Workdesks
Resources	Possible	-
Account definitions	Possible	
Groups of custom target systems	Possible (assigns to all an employee's custom defined target systems user accounts, for which group inheritance is authorized)	-
System entitlements of custom target systems	Possible (assigns to all an employee's custom defined target systems user	-

Assignable Company Resource	Members in Roles	
	Employees	Workdesks
	accounts, for which system entitlement inheritance is authorized)	
Active Directory groups	Possible (assigns to all an employee's Active Directory user accounts and Active Directory contacts, for which Active Directory group inheritance is authorized)	-
SharePoint groups	Possible (assigns to all an employee's SharePoint user accounts for which SharePoint group inheritance is authorized)	-
SharePoint roles	Possible (assigns to all an employee's SharePoint user accounts for which SharePoint role inheritance is authorized)	-
LDAP groups	Possible (assigns to all an employee's LDAP user accounts for which LDAP group inheritance is authorized)	-
Notes groups	Possible (assigns to all an employee's Notes user accounts for which Notes group inheritance is authorized)	-
SAP groups	Possible (assigns to all an employee's SAP user accounts, in the same SAP system and for which SAP group inheritance is authorized)	-
SAP profiles	Possible (assigns to all an employee's SAP user accounts, in the same SAP system and for which SAP profile inheritance is authorized)	-
SAP roles	Possible (assigns to all an employee's SAP user accounts, in the same SAP system and for which SAP role inheritance is authorized)	-
SAP parameters	Possible (assigns to all an employee's SAP user accounts in the same SAP system)	-
Structural profiles	Possible (assigns to all an employee's SAP user accounts, in the same SAP	-

Assignable Company Resource	Members in Roles	
	Employees	Workdesks
	system and for which structural profile inheritance is authorized)	
BI analysis authorizations	Possible (assigns to all an employee's BI user accounts, in the same system and for which group inheritance is authorized)	-
Azure Active Directory groups	Possible (assigns to all an employee's Azure Active Directory user accounts for which Azure Active Directory group inheritance is authorized)	-
Azure Active Directory administrator roles	Possible (assigns to all an employee's Azure Active Directory user accounts for which Azure Active Directory administrator role inheritance is authorized)	-
Azure Active Directory subscriptions	Possible (assigns to all an employee's Azure Active Directory user accounts for which Azure Active Directory subscription inheritance is authorized)	-
Disabled Azure Active Directory service plans	Possible (assigns to all an employee's Azure Active Directory user accounts for which disabled Azure Active Directory service plans inheritance is authorized)	-
Cloud groups	Possible (assigns to all an employee's user accounts for which cloud group inheritance is authorized)	-
Cloud system entitlements	Possible (assigns to all an employee's user accounts for which cloud system entitlement inheritance is authorized)	-
Unix groups	Possible (assigns to all an employee's Unix user accounts for which Unix group inheritance is authorized)	-
E-Business Suite permissions	Possible (assigns to all an employee's E-Business Suite user accounts, in the same E-Business Suite system and for which E-Business Suite group inheritance is authorized)	-
PAM user groups	Possible (assigns to all an employee's PAM user accounts for which PAM group	-

Assignable Company Resource	Members in Roles	
	Employees	Workdesks
	inheritance is authorized)	
Google Workspace products and SKUs	Possible (assigns to all an employee's Google Workspace user accounts, in the same customer and for which Google Workspace products and SKU inheritance is authorized)	-
Google Workspace groups	Possible (assigns to all an employee's Google Workspace user accounts, in the same customer and for which Google Workspace group inheritance is authorized)	-
SharePoint Online groups	Possible (assigns to all an employee's SharePoint Online user accounts for which SharePoint Online group inheritance is authorized)	-
SharePoint Online roles	Possible (assigns to all an employee's SharePoint Online user accounts for which SharePoint Online role inheritance is authorized)	-
Office 365 groups	Possible (assigns to all an employee's Azure Active Directory user accounts for which Office 365 group inheritance is authorized)	-
Exchange Online mail-enabled distribution groups	Possible (assigns to all an employee's Exchange Online mailboxes, Exchange Online mail users and Exchange Online mail contacts for which Exchange Online mail-enabled distribution group inheritance is authorized)	-
System roles	Possible	Possible
Subscribable reports	Possible	-
Software	Possible	Possible

Related topics

- [Assigning company resources to departments, cost centers, and locations](#) on page 82

Permitting assignments of employees, devices, workdesks, and company resources to roles

The default method for assigning company resources is through secondary assignment. For this, employees, devices, and workdesks as well as company resources are added to roles through secondary assignment.

Use role classes to specify how and if employees, devices, workdesks, and company resource are permitted as secondary assignments to roles. Role classes form the basis of mapping hierarchical roles in One Identity Manager. Role classes are used to group similar roles together. The following role classes are available by default in the One Identity Manager:

- Department
- Cost center
- Location
- Application role

Secondary assignment of objects to role in a role class is defined by the following options:

- **Assignments allowed:** This option specifies whether assignments of respective object types to roles of this role class are allowed in general.
- **Direct assignments allowed:** Use this option to specify whether respective object types can be assigned directly to roles of this role class. Set this option if, for example, resources are assigned to departments, cost centers, or locations over the assignment form in the Manager.

NOTE: If this option is not set, the assignment of each object type is only possible through requests in the IT Shop, dynamic roles, or system roles.

Example:

To assign employees directly to a department in the Manager, enable the **Assignment allowed** and the **Direct assignment allowed** options on the **Employees** entry in the **Department** role class.

If employees can only obtain membership in a department through the IT Shop, enable the **Assignment allowed** option but not the **Direct assignment allowed** option on the **Employees** entry in the **Department** role class. A corresponding assignment resource must be available in the IT Shop.

NOTE: Employee, device, workdesk, and company resource assignments are predefined for departments, cost centers, location, and application roles. The configuration of application role assignments cannot be changed.

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
2. Select the **Configure role assignments** task.
3. Use the **Allow assignments** column to specify whether assignment is generally allowed.

NOTE: You can only reset the **Assignment allowed** option if there are no assignments of the respective objects to roles of this role class and none can arise through existing dynamic roles.

4. Use the **Allow direct assignments** column to specify whether a direct assignment is allowed.

NOTE: You can only reset the **Direct assignment allowed** option if there are no direct assignments of the respective objects to roles of this role class.

5. Save the changes.

Blocking inheritance using roles

There are particular cases where you may not want to have inheritance over several hierarchical levels. That is why it is possible to discontinue inheritance within a hierarchy. The effects of this depend on the chosen direction of inheritance.

- Roles marked with the **Block inheritance** option do not inherit any assignments from parent levels in top-down inheritance. It can, however, pass on its own directly assigned company resources to lower level structures.
- In bottom-up inheritance, the role labeled with the **Block inheritance** option inherits all assignments from lower levels in the hierarchy. However, it does not pass any assignments further up the hierarchy.

To discontinue inheritance for departments, cost centers, or locations

1. In the Manager, in the **Organizations** category, select a department, cost center or location.
2. Select the **Change main data** task.
3. Set the **Block inheritance** option.
4. Save the changes.

NOTE: In the case of application roles, inheritance can only be discontinued for custom application roles. For more information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Related topics

- [Discontinuing inheritance](#) on page 13
- [Preventing employees, devices, or workdesks from inheriting individual roles](#) on page 31
- [Preventing inheritance to individual employees, devices, or workdesks](#) on page 31

Preventing employees, devices, or workdesks from inheriting individual roles

Company resource inheritance for single roles can be temporarily prevented. You can use this behavior, for example, to assign all required company resources to a role. Inheritance of company resources does not take place, however, unless inheritance is permitted for the role, for example, by running a defined approval process.

To prevent inheritance for departments, cost centers, or locations

1. In the Manager, in the **Organizations** category, select a department, cost center or location.
2. Select the **Change main data** task.
3. Set one or more of the following options:
 - To prevent employees from inheriting, set the **Employees do not inherit** option.
 - To prevent devices from inheriting, set the **Devices do not inherit** option.
 - To prevent workdesks from inheriting, set the **Workdesks do not inherit** option.
4. Save the changes.

NOTE: This option cannot be configured for application roles. For more information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Related topics

- [Blocking inheritance using roles](#) on page 30
- [Preventing inheritance to individual employees, devices, or workdesks](#) on page 31

Preventing inheritance to individual employees, devices, or workdesks

Inheritance of company resources can be prevented for single employees, devices, or workdesks. You can use this behavior to correct data after importing employees before and

then apply inheritance.

To prevent an employee from inheriting

1. In the Manager, select the employee in the **Employees** category.
2. Select the **Change main data** task.
3. Set the **No inheritance** option.

The employee does not inherit company resources through roles.

NOTE: This option does not have any effect on direct assignments. Company resource direct assignments remain assigned.

4. Save the changes.

To prevent an device from inheriting

1. In the Manager, select the device in the **Devices & Workdesks > Devices** category.
2. Select the **Change main data** task.
3. Set the **No inheritance** option.

The device does not inherit company resources through roles.

NOTE: This option does not have any effect on direct assignments. Company resource direct assignments remain assigned.

4. Save the changes.

To prevent a workdesk from inheriting

1. In the Manager, select the workdesk in the **Devices & Workdesks > Workdesks** category.
2. Select the **Change main data** task.
3. Set the **No inheritance** option.

The workdesk does not inherit company resources through roles.

NOTE: This option does not have any effect on direct assignments. Company resource direct assignments remain assigned.

4. Save the changes.

Related topics

- [Blocking inheritance using roles](#) on page 30
- [Preventing employees, devices, or workdesks from inheriting individual roles](#) on page 31

Inheritance exclusion: Specifying conflicting roles

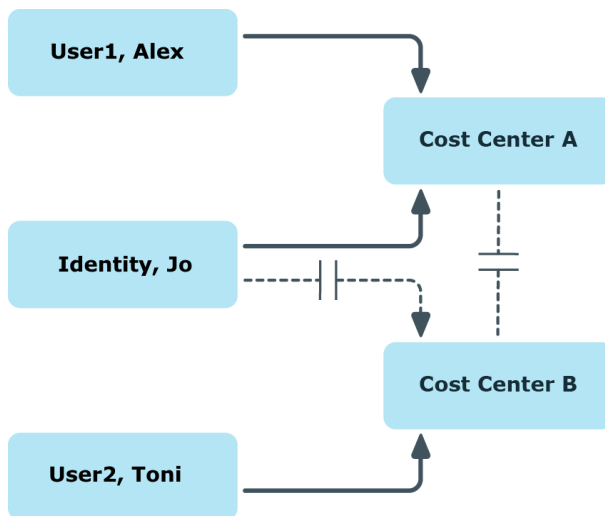
You can define conflicting roles to prevent employees, devices, or workdesks from being assigned to several roles at the same time and from obtaining mutually exclusive company resources through these roles. At the same time, specify which departments, cost centers, and locations are mutually exclusive. This means you may not assign these roles to one and the same employee (device, workdesk).

NOTE: Only roles, which are defined directly as conflicting roles cannot be assigned to the same employee (device, workdesk). Definitions made on parent or child roles do not affect the assignment.

Example:

Cost center B is named as conflicting role to cost center A. Alex User1 and Jo Identity are members of cost center A. Toni User2 is a member of cost center B. Jo Identity cannot be assigned to cost center B. Apart from that, One Identity Manager prevents Alex User1 and Toni User2 from being assigned to cost center A.

Figure 12: Members in conflicting roles



To configure inheritance exclusion

- In the Designer, set the **QER | Structures | ExcludeStructures** configuration parameter and compile the database.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not 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*.

Related topics

- [Specifying inheritance exclusion for departments, cost centers, and locations](#) on page 87

Dynamic roles

Dynamic roles are used to dynamically assign memberships to departments, cost centers, location, business roles, application roles, and IT Shop nodes. Employees, devices, and workdesks are not permanently assigned to these roles, just when they fulfill certain conditions. A check is performed regularly to assess which employees (devices or workdesks) fulfill these conditions. This means the role memberships change dynamically. For example, company resources can be assigned dynamically to all employees in a department in this way; if an employee leaves the department they immediately lose the resources assigned to them.

Example: Dynamic role functionality

All external employees are added to a new dynamic role. These employees should be assigned to a company resource ABC. The dynamic role is initially defined with the following data:

Dynamic role	External employees
Description	All external employees
Object class	PERSON
Condition	IsExternal = 1
Department	A_1

The department A_1 is now assigned the resource ABC. All employees who fulfill the condition at the time the dynamic role was defined are assigned to department A_1 and therefore inherit the resource ABC. Employees who fulfill the condition at a later date, are assigned to department A_1 from that moment. Conversely, employees in department A_1 are removed the moment they are no longer known as external employees by One Identity Manager. The resource ABC is no longer available to those employees assuming they have not been assigned the resource through other channels.

Role memberships through dynamic roles are implemented as indirect, secondary assignments. Therefore secondary assignment of employees, devices, and workdesks to role classes must be permitted. If necessary, further configuration settings need to be made.

Employees can be excluded automatically from dynamic roles on the basis of a denied attestation or a rule violation. An excluded list is maintained to do this. Excluded lists can also be defined for individual employees. In addition, employees can also become members of the role directly or by assignment request or delegation. These memberships are not restricted by the exclusion list.

For more information on automatic exclusion in the event of a denied attestation, see the *One Identity Manager Attestation Administration Guide*. For more information on automatic exclusion in the event of a rule violation, see the *One Identity Manager Web Designer Web Portal User Guide*.

Detailed information about this topic

- [Creating and editing dynamic roles](#) on page 36
- [Tips about conditions for dynamic roles](#) on page 37
- [Testing dynamic role conditions](#) on page 38
- [Calculating role memberships for dynamic roles](#) on page 39
- [Excluding employees from dynamic roles](#) on page 48
- [Displaying the dynamic role overview](#) on page 49
- [Main data for dynamic roles](#) on page 50

Related topics

- [Basic principles for assigning company resources](#) on page 15
- [Permitting assignments of employees, devices, workdesks, and company resources to roles](#) on page 29

Creating and editing dynamic roles

You can create dynamic roles for departments, cost centers, locations, business roles, application roles, and IT Shop nodes. This allows you to specify memberships in these roles.

To create a dynamic role

1. In the Manager, select the role for which you want to create a dynamic role.
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 role for which the dynamic role was created.
2. Open the role's overview form.
3. Select the **Dynamic roles** form element and click on the dynamic role.
4. Select the **Change main data** task.
5. Edit the data and then save the changes.

Related topics

- [Tips about conditions for dynamic roles](#) on page 37
- [Testing dynamic role conditions](#) on page 38
- [Main data for dynamic roles](#) on page 50
- [Creating dynamic roles for departments, cost centers, and locations](#) on page 85

Tips about conditions for dynamic roles

IMPORTANT: If the condition includes a large number of objects to assign, calculating memberships can place a heavy load on the DBQueue Processor and consequently on the database server.

A dynamic role condition is defined as a valid Where clause for database queries and must relate to the selected **Person**, **Hardware**, or **Workdesk** object class.

In the Manager, you have different ways of creating conditions:

- You can enter it directly as an SQL query.
- You can use the Where clause wizard to create the conditions.
- Alternatively, you can enter conditions for employee objects with the filter designer.

NOTE: If you select the **For the account with the target system type** or **For the entitlement with target system type** condition type in the filter designer, only columns that are mapped in Unified Namespace and for which the **Display in the filter designer** column property is enabled can be selected.

Using the @UID_Org variable, you can access the role or organization referenced by the dynamic role.

Example:

The condition for the dynamic role for employees only takes effect if the employee's location (Person.UID_Locality) matches the location of the assigned role or the

```
organization (BaseTree.UID.UID_OrgLocality).
```

Where clause extension:

```
...
```

```
and uid_locality = (select b.UID_OrgLocality from BaseTree b where b.UID_Org  
= @UID_Org)
```

Example:

The condition for the dynamic role for employees is only effective if the assigned role or organization have a certain property.

Where clause extension:

```
...
```

```
and exists (select top 1 1  
from BaseTree b  
where b.UID_Org = @UID_Org  
and b.CustomProperty01 = '123'  
)
```

NOTE: If you add comments to the condition using the comment characters --, // or %, the DBQueue Processor cannot correctly calculate the dynamic role. The calculation quits with an error. Always use the comment characters /* ... */ to enclose comments.

Related topics

- [Testing dynamic role conditions](#) on page 38


Testing dynamic role conditions

NOTE: To perform the task, users require the **Common_AllowRiskyWhereClauses** program function.

NOTE: This task is only visible when the dynamic role condition is displayed as an SQL query.

You should test which objects fulfill the given condition before you save a dynamic role.

To test the SQL condition for a dynamic role

1. In the Manager, select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select **Change main data**.
5. Click  (**Edit SQL**) on the form.
This displays the condition as SQL query.
6. Select the **Test condition** task.
On the main data form, in the **Test result** field, all objects determined by the condition are displayed.

Related topics

- [Tips about conditions for dynamic roles](#) on page 37

Calculating role memberships for dynamic roles

To calculate the role memberships, One Identity Manager tests every dynamic role to ensure that:

- There is at least one object that satisfies the condition but is not assigned to the role
- There is at least one object that does not satisfy the condition but is assigned to the role
- The exclusion list was changed

If one of the conditions is fulfilled, a request to add or delete memberships is sent to the DBQueue Processor.

NOTE: When the dynamic roles are tested, employee objects that are marked for deletion are:

- Not added to roles through dynamic roles even if the miscellaneous condition is fulfilled.
- Removed from the role even if the miscellaneous condition should be fulfilled

The calculation of role memberships in dynamic roles can be triggered by different methods.

- Cyclical checking using a schedule
- Recalculation when objects are changed
- Start recalculation manually

Related topics

- [Schedules for calculating dynamic roles on page 40](#)
- [Calculating dynamic roles immediately if objects change on page 44](#)
- [Calculating role memberships for dynamic roles immediately on page 47](#)
- [Excluding dynamic roles from recalculation on page 47](#)
- [Excluding employees from dynamic roles on page 48](#)

Schedules for calculating dynamic roles

NOTE: When a schedule is started, all dynamic roles that have this schedule assigned and where the **No recalculation of assignments** option is not set are recalculated.

In the standard installation of One Identity Manager, the **Dynamic roles check** schedule is already defined. This schedule is used when creating a new dynamic role. All dynamic role memberships are checked using this schedule and recalculation tasks are sent to the DBQueue Processor if necessary. Checks are made at predefined intervals. If necessary, you can change the default schedule for dynamic roles or create new schedules.

For more information about schedules, see the *One Identity Manager Operational Guide*.

Related topics

- [Creating and editing dynamic role schedules on page 40](#)
- [Starting dynamic role schedules immediately on page 43](#)
- [Assigning dynamic roles to schedules on page 43](#)
- [Calculating dynamic roles immediately if objects change on page 44](#)
- [Editing properties for immediate recalculation on page 46](#)
- [Calculating role memberships for dynamic roles immediately on page 47](#)
- [Main data for dynamic roles on page 50](#)

Creating and editing dynamic role schedules


If necessary, you can change the default schedule for dynamic roles or create new schedules.

To edit a schedule

1. In the Manager, select the **Organizations > Basic configuration data > Schedules** category.
The result list shows all the schedules configured for dynamic roles.
2. Select a schedule in the result list and run the **Change main data** task.

3. Edit the schedule's main data.
4. Save the changes.

To create a schedule

1. In the Manager, select the **Organizations > Basic configuration data > Schedules** category.
2. Click  in the result list.
3. Edit the schedule's main data.
4. Save the changes.

Edit the following schedule properties.

Table 5: Schedule properties

Property	Meaning
Name	Schedule ID.
Description	Detailed description of the schedule.
Enabled	Specifies whether the schedule is enabled.
Time zones	Unique identifier for the time zone that is used for running the schedule. Choose between Universal Time Code or one of the time zones in the menu.
Start (date)	The day on which the schedule should be run for the first time. If this day conflicts with the defined interval type, the first run is on the next available day based on the start date.
Validity period	Period within which the schedule is run. <ul style="list-style-type: none"> • If the schedule will be run for an unlimited period, select the Unlimited duration option. • To set a validity period, select the Limited duration option and enter the day the schedule will be run for the last time in End (date).
Occurs	Interval in which the task is run. Other settings may be required depending on the settings. <ul style="list-style-type: none"> • Hourly: The schedule is run at defined intervals of a multiple of hours such as every two hours. <ul style="list-style-type: none"> • Under Repeat every, specify after how many hours the schedule is run again. • The starting point is calculated from the rate of occurrence and the interval type. • Daily: The schedule is run at specified times in a defined interval of days such as every second day at 6am and 6pm.

Property	Meaning
----------	---------

- | | |
|-------------------|--|
| | <ul style="list-style-type: none"> Under Start time, specify the times to run the schedule. Under Repeat every, specify after how many days the schedule is run again. |
| • Weekly : | <p>The schedule is run at a defined interval of weeks, on a specific day, at a specified time such as every second week on Monday at 6am and 6pm.</p> <ul style="list-style-type: none"> Under Start time, specify the times to run the schedule. Under Repeat every, specify after how many weeks the schedule is run again. Specify the set day of the week for running the schedule. |
| • Weekly : | <p>The schedule is run at a defined interval of months, on a specific day, at a specified time such as every second month on the 1st and the 15th at 6am and 6pm.</p> <ul style="list-style-type: none"> Under Start time, specify the times to run the schedule. Under Repeat every, specify after how many months the schedule is run again. Specify the days of the month (1st - 31st of the month). |

NOTE: If the **Monthly** interval type with the sub interval **29, 30** or **31** does not exist in this month, the last day of the month is used.

Example:

A schedule that is run on the 31st day of each month is run on April 30th. In February, the schedule is run on the 28th (or 29th in leap year).

- | | |
|-------------------|--|
| • Yearly : | <p>The schedule is run at a defined interval of years, on a specific day, at a specified time such as every year on the 1st, the 100th, and the 200th day at 6am and 6pm.</p> <ul style="list-style-type: none"> Under Start time, specify the times to run the schedule. Under Repeat every, specify after how many years the schedule is run again. Specify the days of the year (1st - 366th day of the year). |
|-------------------|--|

NOTE: If you select the 366th day of the year, the schedule is only run in leap years.

- | | |
|---|---|
| • Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday : | <p>The schedule is run on a defined day of the week, in specified months, at specified times such as every second Saturday in January and June at 10am.</p> <ul style="list-style-type: none"> Under Start time, specify the times to run the schedule. |
|---|---|

Property	Meaning
	<ul style="list-style-type: none"> Under Repeat every, specify after how many days of the month the schedule is run again. The values 1 to 4, -1 (last day of the week), and -2 (last day but one of the week) are permitted. Specify in which month to run the schedule. The values 1 to 12 are permitted. If the value is empty, the schedule is run each month.
Start time	Fixed start time Enter the time in local format for the chosen time zone. If there is a list of start times, the schedule is started at each of the given times.
Repeat every	Rate of occurrence for running the schedule within the selected time interval.

Related topics

- [Assigning dynamic roles to schedules](#) on page 43
- [Starting dynamic role schedules immediately](#) on page 43
- [Main data for dynamic roles](#) on page 50

Starting dynamic role schedules immediately

NOTE: When a schedule is started, all dynamic roles that have this schedule assigned and where the **No recalculation of assignments** option is not set are recalculated.

To start a schedule immediately

1. In the Manager, select the **Organizations > Basic configuration data > Schedules** category.
2. Select the schedule in the result list.
3. Select the **Start immediately** task.

A message appears confirming that the schedule was started.

Assigning dynamic roles to schedules

Use this task to assign dynamic roles to the selected schedule that will run them. The assignment form displays all the dynamic roles that are assigned this selected schedule.

To assign dynamic roles to a schedule

1. In the Manager, select the **Organizations > Basic configuration data > Schedules** category.
2. Select the schedule in the result list.
3. Select the **Assign dynamic roles** task.
4. In the **Add assignments** pane, double-click the dynamic roles you want to assign.
5. Save the changes.

To change an assignment

1. In the Manager, select the **Organizations > Basic configuration data > Schedules** category.
2. Select the schedule in the result list.
3. Select the **Assign dynamic roles** task.
4. Select the **Show objects already assigned to other objects** menu item in the assignment form's context menu.
This shows dynamic roles that are already assigned to other schedules.
5. In the **Add assignments** pane, double-click on one of these dynamic roles.
This dynamic role is assigned to the currently selected schedule.
6. Save the changes.

NOTE: Assignments cannot be removed. Dynamic roles must be assigned a schedule. It is compulsory.

Related topics

- [Main data for dynamic roles](#) on page 50

Calculating dynamic roles immediately if objects change

Memberships can be checked immediately by the DBQueue Processor and changed as necessary when object properties are changed. For each dynamic role, you can define which properties trigger a recalculation of role memberships if they are changed.

Requirements for immediate recalculation

- The configuration parameters for immediate recalculation are set. Check the following configuration parameters in the Designer and set them if necessary.

- **QER | Structures | DynamicGroupCheck:** The configuration parameter controls the generation of calculation tasks for dynamic roles.
If the configuration parameter is not set, the subparameters do not apply.
- **QER | Structures | DynamicGroupCheck | CalculateImmediatelyPerson:** If the configuration parameter is set, a calculation task is immediately queued for the DBQueue Processor when changes are made to employees or employee-related objects.
- **QER | Structures | DynamicGroupCheck | CalculateImmediatelyHardware:** If the configuration parameter is set, a calculation task is immediately queued for the DBQueue Processor when changes are made to devices or device-related objects.
- **QER | Structures | DynamicGroupCheck | CalculateImmediatelyWorkdesk:** If the configuration parameter is set, a calculation task is immediately queued for the DBQueue Processor when changes are made to workstations or workstation-related objects.
- The **Immediate recalculation of assignments** option is enabled for the dynamic roles. The properties that trigger recalculation are defined.
- The **No recalculation of assignments** option is not enabled for the dynamic roles.

To enable immediate recalculation of a dynamic role

1. In the Manager, select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select the **Change main data** task.
5. Enable the **Immediate recalculation of assignments** option.
6. On the **Recalculation properties** tab, add the properties that trigger recalculation of the dynamic role.
 - a. Click **Add**.
 - b. Next to the **Property** field, click ➔.
 - c. Under **Property**, select the table and column to trigger recalculation.
 - d. Click **OK**.
 - e. Repeat these steps for all properties.
7. Save the changes.

Related topics

- [Editing properties for immediate recalculation](#) on page 46
- [Main data for dynamic roles](#) on page 50
- [Calculating role memberships for dynamic roles](#) on page 39
- [Calculating role memberships for dynamic roles immediately](#) on page 47

Editing properties for immediate recalculation

For individual dynamic roles, you can define which properties trigger a recalculation of role memberships if they are changed.

To add a property

1. In the Manager, select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select the **Change main data** task.
5. On the **Recalculation Properties** tab, add the properties.
 - a. Click **Add**.
 - b. Next to the **Property** field, click ➔.
 - c. Under **Property**, select the table and column to trigger recalculation.
 - d. Click **OK**.
6. Save the changes.

To disable a property

1. In the Manager, select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select the **Change main data** task.
5. On the **Recalculation properties** tab, select the column in the list and check the **Disabled** option.
6. Save the changes.

To remove a property

1. In the Manager, select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select the **Change main data** task.
5. On the **Recalculation Properties** tab, select the column in the list and click **Remove**.
6. Save the changes.

Calculating role memberships for dynamic roles immediately

You can make a single dynamic role calculation immediately

To calculate role membership immediately

1. In the Manager, select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select the **Change main data** task.
5. Select the **Start recalculation immediately** task and close the prompt with **OK**.
A processing task for the DBQueue Processor is set in the DBQueue.

Related topics

- [Calculating role memberships for dynamic roles on page 39](#)
- [Calculating dynamic roles immediately if objects change on page 44](#)
- [Editing properties for immediate recalculation on page 46](#)

Excluding dynamic roles from recalculation

You can exclude individual dynamic roles from recalculation. In this case, role memberships are not automatically recalculated. Existing role memberships remain as they are.

To exclude a dynamic role from recalculation

1. In the Manager, select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select the **Change main data** task.
5. Enable the **No recalculation of assignments** option.
6. Save the changes.

Related topics

- [Calculating role memberships for dynamic roles on page 39](#)
- [Main data for dynamic roles on page 50](#)

Excluding employees from dynamic roles

Employees can be excluded automatically from dynamic roles on the basis of a denied attestation or a rule violation. An excluded list is maintained to do this. Excluded lists can also be defined for individual employees.

To add an employee to the excluded list

1. In the Manager, select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select the **Exclude employees** task.
5. Click **Add** and select the employee from the **Employee** menu.
6. (Optional) Enter a reason for the exclusion.
7. Save the changes.

Related topics

- [Main data of exclude lists for dynamic roles](#) on page 49
- [Removing employees from the exclusion list](#) on page 48
- [Dynamic roles with incorrectly excluded employees](#) on page 86

Removing employees from the exclusion list

To remove an employee from the exclusion list

1. In the Manager, select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select the **Exclude employees** task.
5. Select the employee and click **Remove**.
6. Save the changes.

Related topics

- [Main data of exclude lists for dynamic roles](#) on page 49
- [Excluding employees from dynamic roles](#) on page 48

Main data of exclude lists for dynamic roles

The following main data is displayed for an employee in the exclusion list of a dynamic role.

Table 6: Main data of exclude lists for dynamic roles

Property	Description
Employee	Unique identifier of the excluded employee.
Description	Reason for excluding the employee. If the employee is excluded because attestation was denied or due to a rule violation, a standard reason is entered here.
Condition not applicable	<p>Specifies whether the dynamic role condition applies to the excluded person. If the option is disabled, the condition applies.</p> <p>TIP: If the option is enabled, the employee can be removed from the exclusion list. For more information, see Removing employees from the exclusion list on page 48.</p>
Not assigned by dynamic role	<p>Specifies whether the excluded employee is still assigned to the role by another way.</p> <p>Employees can, in addition, also become members of the role directly or by assignment request or delegation. The exclusion list does not influence these assignments.</p>

Related topics

- [Excluding employees from dynamic roles](#) on page 48
- [Removing employees from the exclusion list](#) on page 48
- [Dynamic roles with incorrectly excluded employees](#) on page 86

Displaying the dynamic role overview

You can see the most important information about a dynamic role on the overview form.

To obtain an overview of a dynamic role


1. In the Manager, select the role for which the dynamic role was created. The department, for example.
2. Open the role's overview form.
3. Select **Dynamic roles** and click on the dynamic role.
4. Select the **Dynamic role overview** task.
5. Select the report **Show overview**.

The report provides a summary of key information about a dynamic role, including the schedule, excluded employees, and recalculation properties.

Main data for dynamic roles

Enter the following data for a dynamic role.

Table 7: Dynamic role main data

Property	Description
Role/Organization	Role (department, cost center, location, business role, IT Shop node, application node) referenced by the dynamic role. This data is preset with the selected role.
Object class	Object class that the dynamic role applies to. Choose between Person , Hardware , and Workdesk . NOTE: The combination of object class and role must be unique. It is not possible that two dynamic roles from the same object class to refer to one role.
Dynamic role	Name of the dynamic role.
Calculation schedule	Schedule, which triggers cyclical recalculation of the role membership. To create a schedule, click  . Enter the schedule's main data.
Description	Text field for additional explanation.
Condition	Defines which objects of the object class become members of the selected role. For more information, see Tips about conditions for dynamic roles on page 37. For more information, see Tips about conditions for dynamic roles on page 37.
No recalculation of assignments	Specifies whether to recalculate memberships. If the option is enabled, role memberships will not be recalculated automatically. Existing role memberships remain as they are.
Immediate recalculation of assignments	Specifies whether the dynamic role is recalculated if changes are made to specified properties. If the option is enabled, specify the properties for recalculation.
Recalculation property: Property	Property whose change triggers an immediate recalculation of the dynamic role.
Recalculation property: Disabled	Specifies whether immediate recalculation of the property is disabled.

Related topics

- [Creating and editing dynamic roles on page 36](#)
- [Testing dynamic role conditions on page 38](#)
- [Schedules for calculating dynamic roles on page 40](#)
- [Assigning dynamic roles to schedules on page 43](#)
- [Calculating role memberships for dynamic roles immediately on page 47](#)
- [Excluding dynamic roles from recalculation on page 47](#)

Departments, cost centers, and locations

Departments, cost centers, locations, and business roles are each mapped to their own hierarchy under **Organizations**. This is due to their special significance for daily work schedules in many companies. Various company resources can be assigned to organizations, for example, permissions in different SAP systems or Azure Active Directory tenants. You can add employees to single roles as members. Employees obtain their company resources through these assignments when the One Identity Manager is appropriately configured.

Detailed information about this topic

- [One Identity Manager users for managing departments, cost centers, and locations on page 53](#)
- [Basic information for departments, cost centers, and locations on page 55](#)
- [Creating and editing departments on page 63](#)
- [Creating and editing cost centers on page 67](#)
- [Creating and editing locations on page 71](#)
- [Setting up IT operating data for departments, cost centers, and locations on page 76](#)
- [Preparing hierarchical roles for company resource assignments on page 24](#)
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations on page 81](#)
- [Assigning company resources to departments, cost centers, and locations on page 82](#)
- [Creating dynamic roles for departments, cost centers, and locations on page 85](#)
- [Assign organizations on page 86](#)
- [Specifying inheritance exclusion for departments, cost centers, and locations on page 87](#)
- [Assigning extended properties to departments, cost centers, and locations on page 89](#)
- [Reports about departments, cost centers, and locations on page 91](#)

- [Configuration parameters for managing departments, cost centers, and locations](#) on page 209

One Identity Manager users for managing departments, cost centers, and locations

The following users are used for the administration of departments, cost centers, and locations.

Table 8: Users

User	Tasks
Administrators for organizations	<p>Administrators must be assigned to the Identity Management Organizations Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Set up and edit departments, cost centers, and locations. • Assign company resources to departments, cost centers, and locations. • Attest the main data of departments, cost centers, and locations. • Administrate application roles for role approvers, role approvers (IT), and attestors. • Set up other application roles as required.
Additional managers	<p>The additional managers must be assigned to the Identity Management Organizations Additional managers application role or to a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Have permission to manage departments, cost centers and locations.
Approvers for organizations	<p>Attestors must be assigned to the Identity Management Organizations Attestors application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Attest correct assignment of company resources to departments, cost centers, and locations for which they are responsible. • Can view main data for departments, cost centers, and locations but cannot edit them.

NOTE: This application role is available if the module Attestation

User	Tasks
	<p>Module is installed.</p>
Approvers for organizations	<p>Role approvers must be assigned to the Identity Management Organizations Role approvers application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Are approvers for the IT Shop. • Approve request from departments, cost centers, and locations for which they are responsible.
Approvers (IT) for organizations	<p>IT role approvers must be assigned to the Identity Management Organizations Role approvers (IT) application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Are IT role approvers for the IT Shop. • Approve request from departments, cost centers, and locations for which they are responsible.
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> • 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. • Create and configure password policies as required.

Basic information for departments, cost centers, and locations

The following basic information is relevant for building up hierarchical roles in One Identity Manager.

- Configuration parameters

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for different configuration parameters. Check the configuration parameters and modify them as necessary to suit your requirements.

Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.

- Role classes

Role classes form the basis of mapping hierarchical roles in One Identity Manager. Role classes are used to group similar roles together.

- Role types

Create role types in order to classify roles. Roles types can be used to map roles in the user interface, for example.

- Functional areas

To analyze rule checks for different areas of your company in the context of identity audit, you can set up functional areas. Functional areas can be assigned to roles. You can enter criteria that provide information about risks from rule violations for functional areas and roles. Moreover, functional areas can be used during peer group analysis of requests or attestation cases.

- Attestors

In One Identity Manager you can assign departments, cost centers, and locations to employees who can be brought in as attestors in attestation cases, provided that the approval workflow is set up accordingly. To do this, assign the departments, cost centers, and locations to application roles for attestors. 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*.

- Role approvers and role approvers (IT)

In One Identity Manager you can assign departments, cost centers and locations to employees who can be brought in as approvers in approval processes for IT Shop requests, provided that the approval workflow is set up accordingly. To do this, assign the departments, cost centers, and locations to application roles for role approvers. For more information, see the *One Identity Manager IT Shop*

Administration Guide.

Default application roles for approvers and approvers (IT) are available in One Identity Manager. You may create other application roles as required. For more information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Detailed information about this topic

- [Role classes for departments, cost centers, and locations](#) on page 56
- [Role types for departments, cost centers, and locations](#) on page 57
- [Functional areas for departments, cost centers, and locations](#) on page 59
- [Attestors for departments, cost centers, and locations](#) on page 61
- [Approvers and approvers \(IT\) for departments, cost centers, and locations](#) on page 62
- [Configuration parameters for managing departments, cost centers, and locations](#) on page 209

Role classes for departments, cost centers, and locations

Role classes form the basis of mapping hierarchical roles in One Identity Manager. Role classes are used to group similar roles together. The direction of inheritance is specified by the role class. In addition, assignments that are allowed to be made to individual roles of this role class are specified in a role class.

The following role classes are provided by default for mapping organizations in One Identity Manager:

- Department
- Cost center
- Location

Top down inheritance is defined for departments, cost centers, locations, and application roles. Employees, devices, workdesks, and company resource assignments are predefined for departments, cost centers, and locations. You can edit these role class assignments.

Related topics

- [Inheritance directions within a hierarchy](#) on page 11
- [Permitting assignments of employees, devices, workdesks, and company resources to roles](#) on page 29


Assigning role types to role classes for departments, cost centers, and locations

To assign a role type to a role class

1. In the Manager, select the **Organizations > Basic configuration data > Role classes** category.
2. In the result list, select the role class.
3. Select the **Assign role types** task.
4. In the **Add assignments** pane, assign role types.

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

To remove an assignment

- Select the role type and click .

Related topics

- [Role types for departments, cost centers, and locations](#) on page 57
- [Creating role types for departments, cost centers, and locations](#) on page 58
- [Assigning role classes to role types for departments, cost centers, and locations](#) on page 59

Role types for departments, cost centers, and locations

To achieve better classification, you can define role types and assign them to role classes and roles. The following restrictions apply:

- You can assign a role type to several role classes.
- If you assign role types to a role class you can only select these role types for the roles of this role class. Other role types are not available for selection.
- If you do not assign a role type to a role class, you can only use role types that are not assigned to any other role class for roles in this role class.
- The **Business role** role type is predefined. This role type cannot be assigned to the **Department**, **Cost center**, or **Location** role classes. Assign this role type to role classes that map business roles.



Example:

The **Business role** role type is predefined. The **Region**, **Country**, **Sales**, and **Development** role types are also created.

- The **Business roles** role type is assigned to the **External projects** role class.
The **Business roles** role type can also be given to roles of this role class.
- The **Business roles**, **Region**, and **Country** role types are assigned to the **Employee** role class.
The **Business roles**, **Region**, and **Country** role types can also be given to roles of this role class.
- The **Region** and **Country** role types are assigned to the **Location** role class.
The **Region** and **Country** role types can also be given locations.
- The **Cost center** and **Department** role classes are not assigned any role types.
The **Sales** and **Development** role types can also be given to cost centers and departments.

Creating role types for departments, cost centers, and locations

To create role types

1. In the Manager, select the **Organizations > Basic configuration data > Role types** category.
2. Click  in the result list.
3. Enter the following information:
 - **Role type:** Role type name. Translate the given text using the  button.
 - **Description:** (Optional) Text field for additional explanation.
 - **No multiple assignment of employees:** This option does not work for departments, cost centers, and locations.
4. Save the changes.


Assigning role classes to role types for departments, cost centers, and locations

To assign role classes to a role type

1. In the Manager, select the **Organizations > Basic configuration data > Role types** category.
2. Select the role type in the result list.
3. Select the **Assign role classes** task.
4. 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 .
5. Save the changes.

Related topics

- [Role types for departments, cost centers, and locations](#) on page 57
- [Assigning role types to role classes for departments, cost centers, and locations](#) on page 57

Functional areas for departments, cost centers, and locations

To analyze rule checks for different areas of your company in the context of identity audit, you can set up functional areas. Functional areas can be assigned to hierarchical roles and service items. You can enter criteria that provide information about risks from rule violations for functional areas and hierarchical roles. To do this, you specify how many rule violations are permitted in a functional area or a 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 cost centers. Proceed as follows:

1. Set up functional areas.
2. Assign cost centers to the functional areas.
3. Define assessment criteria for the cost centers.
4. Specify the number of rule violations allowed for the functional area.
5. Assign compliance rules required for the analysis to the functional area.
6. 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 **Organizations > 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 9: Functional area properties

Property	Description
Functional area	Description of the functional area
Parent Functional area	Parent functional area in a hierarchy. 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.

For more detailed information about rule checking, see the *One Identity Manager Compliance Rules Administration Guide*. For more information about peer group analysis, see the *One Identity Manager IT Shop Administration Guide* and the *One Identity Manager Attestation Administration Guide*.

Attestors for departments, cost centers, and locations

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

In One Identity Manager you can assign departments, cost centers, and locations to employees who can be brought in as attestors in attestation cases, provided that the approval workflow is set up accordingly. To do this, assign the departments, cost centers, and locations to application roles for attestors. 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 10: Default application roles for attestors


User	Tasks
Approvers for organizations	<p>Attestors must be assigned to the Identity Management Organizations Attestors application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Attest correct assignment of company resources to departments, cost centers, and locations for which they are responsible.• Can view main data for departments, cost centers, and locations but cannot edit them. <p>NOTE: This application role is available if the module Attestation Module is installed.</p>

To add employees to default application roles for attestors

1. In the Manager, select the **Organizations > Basic configuration data > Attestors** category.
2. Select the **Assign employees** task.
3. In the **Add assignments** pane, add employees.

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

To remove an assignment

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

Approvers and approvers (IT) for departments, cost centers, and locations

In One Identity Manager you can assign departments, cost centers and locations to employees who can be brought in as approvers in approval processes for IT Shop requests, provided that the approval workflow is set up accordingly. To do this, assign the departments, cost centers, and locations to application roles for role approvers. For more information, see the *One Identity Manager IT Shop Administration Guide*.

Default application roles for approvers and approvers (IT) are available in One Identity Manager. You may create other application roles as required. For more information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 11: Default application roles for approvers


User	Tasks
Approvers for organizations	<p>Role approvers must be assigned to the Identity Management Organizations Role approvers application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Are approvers for the IT Shop.• Approve request from departments, cost centers, and locations for which they are responsible.
Approvers (IT) for organizations	<p>IT role approvers must be assigned to the Identity Management Organizations Role approvers (IT) application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Are IT role approvers for the IT Shop.• Approve request from departments, cost centers, and locations for which they are responsible.

To specify a role approver or role approver (IT)

1. In the Manager, select the **Organizations > Basic configuration data > Role approvers** category.
- OR -
In the Manager, select the **Organizations > Basic configuration data > Role approvers (IT)** category.
2. Select the **Assign employees** task.
3. In the **Add assignments** pane, add employees.


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

To remove an assignment

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

Creating and editing departments

To create or edit a department

1. In the Manager, select the **Organizations > Departments** category.
2. In the result list, select a department and run the **Change main data** task.
 - OR -
 - Click  in the result list.
3. Edit the department's main data.
4. Save the changes.


Detailed information about this topic






- [General main data for departments](#) on page 63
- [Contact data for departments](#) on page 66
- [Functional area and risk assessment for departments](#) on page 66
- [Setting up IT operating data for departments, cost centers, and locations](#) on page 76

General main data for departments

Enter the following data for a department.

Table 12: General main data of a department

Property	Description
Department	Name of the department Translate the given text using the  button.
Short name	Short name of the department
Object ID	Unique department object ID. The object ID is required, for example, in SAP systems for assigning employees to departments.
Parent department	Parent of department in the hierarchy. To organize departments hierarchically, select the parent department in

Property	Description
	the menu. Leave this field empty if the department is at the top level of the department hierarchy.
Full name	Complete name of the department including parent departments. Translate the given text using the  button.
Role type	Role types for more detailed classification.
Location	Location to which the department is primary assigned.
Manager	Manager responsible for the department.
2nd Manager	Assistant manager of the department.
Additional manager	<p>Application role for a group of managers and deputies who manage this department.</p> <p>To create a new application role, click . Enter the application role name and assign a parent application role.</p>
Attestors	<p>Applications role whose members are authorized to approve attestation cases for this department.</p> <p>To create a new application role, click . Enter the application role name and assign a parent application role.</p> <p> NOTE: This property is available if the Attestation Module is installed.</p>
Cost center	Cost center to which the department is primary assigned.
Role approver	<p>Application role whose members approve IT Shop requests for members of this department.</p> <p>To create a new application role, click . Enter the application role name and assign a parent application role.</p>
Role approver (IT)	<p>Application role whose members approve IT Shop requests for members of this department.</p> <p>To create a new application role, click . Enter the application role name and assign a parent application role.</p>
Description	Text field for additional explanation.
Comment	Text field for additional explanation.
Remarks	Text field for additional explanation.
Certification status	<p>Certification status of the department. You can select the following certification statuses:</p> <ul style="list-style-type: none"> • New: The department was newly added to the One Identity Manager database. • Certified: The department main data was granted approval by

Property	Description
	<p>the manager.</p> <ul style="list-style-type: none"> • Denied: The department data was denied approval by the manager. <p>The certification status can be set depending on the result of regular attestations.</p>
Import data source	Target system or data source, from which the data set was imported.
Full name	Full name of the department include parent departments.
Deactivated	Specifies whether the department is actively used. Set this option if the department is not used. This option does not have any effect on the calculation of inheritance.
Block inheritance	Specifies whether inheritance for this department can be discontinued. Set this option to discontinue inheritance within the department hierarchy.
X500 nodes	Select this option to label a department for exporting to an X500 schema.
Employees do not inherit	Specifies whether employee inheritance should be temporarily prevented for this department.
Devices do not inherit	Specifies whether device inheritance should be temporarily prevented for this department.
Workdesks do not inherit	Specifies whether workdesk inheritance should be temporarily prevented for this department.
Dynamic roles not allowed	Specifies whether a dynamic role can be created for the department.
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.
Spare date no. 01 ... Spare date no. 03	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Related topics

- [Role types for departments, cost centers, and locations](#) on page 57
- [Attestors for departments, cost centers, and locations](#) on page 61
- [Approvers and approvers \(IT\) for departments, cost centers, and locations](#) on page 62
- [Blocking inheritance using roles](#) on page 30

- [Preventing employees, devices, or workdesks from inheriting individual roles](#) on page 31
- [Creating dynamic roles for departments, cost centers, and locations](#) on page 85
- [Certifying departments, cost centers, and locations](#) on page 90

Contact data for departments

Enter the following contact data for departments. Select the  button next to the input field to activate it and add data. Use the  button to remove data from a list.

Table 13: Contact data for departments

Property	Description
Email addresses	Email addresses for the department.
Visitors address	Department address for visitors.
Visiting hours	Department hours for visitors.
Phone hours	Department telephone hours.
Business hours	Department business hours.
Zip code	Department's zip code.

Functional area and risk assessment for departments

Here, you can enter values to classify the department, which analyzes the risk of a department with respect to identity audit.

Table 14: Main data of a department's functional area

Property	Description
Country	Country. You require this to determine the employee's language and working hours.
State	State. You require this to determine the employee's language and working hours.
Functional area	Department functional area. This data is required for department's risk assessment.
Risk index (calculated)	A risk index is calculated for the department risk assessment based on assigned company resources. This field is only visible if the QER


Property	Description
	CalculateRiskIndex configuration parameter is set. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Transparency index	Specifies how well you can trace department assignments. Use the slider to enter a value between 0 and 1 . 0 : no transparency 1 : full transparency
Max. number of rule violations	Number of rule violations allowed in this department. The value can be evaluated when compliance rules are checked. For more information, see the <i>One Identity Manager Compliance Rules Administration Guide</i> . NOTE: This property is only available if the Compliance Rules Module is installed.
Turnover for this unit	Turnover for this department.
Earnings for this unit	Earnings for this department.

Related topics

- [Determining the language for employees](#) on page 148
- [Determining employees working hours](#) on page 149
- [Functional areas for departments, cost centers, and locations](#) on page 59

Creating and editing cost centers

To create or edit a cost center

1. In the Manager, select the **Organizations > Cost centers** category.
2. In the result list, select a cost center and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the cost center's main data.
4. Save the changes.

Detailed information about this topic






- [General main data for cost centers](#) on page 68
- [Functional area and risk assessment for cost centers](#) on page 70


- [Setting up IT operating data for departments, cost centers, and locations](#) on page 76

General main data for cost centers

Enter the following data for a cost center.

Table 15: General main data of a cost center

Property	Description
Cost center	Cost center name. Translate the given text using the  button.
Short name	Cost center short name.
Parent cost center	Parent of cost center in the hierarchy. To organize cost centers hierarchically, select the parent cost center in the menu. Leave this field empty if the cost center is at the top level of the cost center hierarchy.
Full name	Complete name of the cost center including parent cost centers. Translate the given text using the  button.
Role type	Role types for more detailed classification.
Manager	Manager responsible for the cost center.
2nd Manager	Deputy cost center manager.
Additional manager	Application role for a group of managers and deputies who manage this cost center. To create a new application role, click  . Enter the application role name and assign a parent application role.
Attestors	Applications role whose members are authorized to approve attestation cases for this cost center. 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.
Department	Department to which the cost center is primary assigned.
Location	Location to which the cost center is primary assigned.
Role approver	Application role whose members approve IT Shop requests for members of this cost center. To create a new application role, click  . Enter the application role name and assign a parent application role.
Role approver (IT)	Application role whose members approve IT Shop requests for members of this cost center.

Property	Description
	To create a new application role, click  . Enter the application role name and assign a parent application role.
Description	Text field for additional explanation.
Comment	Text field for additional explanation.
Remarks	Text field for additional explanation.
Certification status	<p>Certification status of the cost center. You can select the following certification statuses:</p> <ul style="list-style-type: none"> • New: The cost center was newly added to the One Identity Manager database. • Certified: The cost center main data was granted approval by the manager. • Denied: The cost center main data was denied approval by the manager. <p>The certification status can be set depending on the result of regular attestations.</p>
Import data source	Target system or data source, from which the data set was imported.
Deactivated	Specifies whether the cost center is actively used. Set this option if the cost center is not used. This option does not have any effect on the calculation of inheritance.
Block inheritance	Specifies whether inheritance for this cost center can be discontinued. Set this option to discontinue inheritance within the cost center hierarchy.
X500 nodes	Select this option to label a cost center for exporting to an X500 schema.
Employees do not inherit	Specifies whether employee inheritance should be temporarily prevented for this cost center.
Devices do not inherit	Specifies whether device inheritance should be temporarily prevented for this cost center.
Workdesks do not inherit	Specifies whether workdesk inheritance should be temporarily prevented for this cost center.
Dynamic roles not allowed	Specifies whether a dynamic role can be created for the cost center.
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.

Property	Description
Spare date no. 01 ... Spare field no. 03	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Related topics

- [Role types for departments, cost centers, and locations](#) on page 57
- [Attestors for departments, cost centers, and locations](#) on page 61
- [Approvers and approvers \(IT\) for departments, cost centers, and locations](#) on page 62
- [Blocking inheritance using roles](#) on page 30
- [Preventing employees, devices, or workdesks from inheriting individual roles](#) on page 31
- [Creating dynamic roles for departments, cost centers, and locations](#) on page 85
- [Certifying departments, cost centers, and locations](#) on page 90

Functional area and risk assessment for cost centers

Here, you can enter values to classify the cost center, which analyzes the risk of a cost center with respect to identity audit.

Table 16: Main data of a cost center's functional area

Property	Description
Country	Country. You require this to determine the employee's language and working hours.
State	State. You require this to determine the employee's language and working hours.
Functional area	Cost center's function area. This data is required for cost center's risk assessment.
Risk index (calculated)	A risk index is calculated for the cost center risk assessment based on assigned company resources. This field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Transparency index	Specifies how well you can trace cost center assignments. Use the slider to enter a value between 0 and 1 .


Property	Description
	0 : no transparency 1 : full transparency
Max. number of rule violations	Number of rule violations allowed in this cost center. The value can be evaluated when compliance rules are checked. For more information, see the <i>One Identity Manager Compliance Rules Administration Guide</i> . NOTE: This property is only available if the Compliance Rules Module is installed.
Turnover for this unit	Turnover for the cost center.
Earnings for this unit	Earnings for the cost center.

Related topics

- [Determining the language for employees](#) on page 148
- [Determining employees working hours](#) on page 149
- [Functional areas for departments, cost centers, and locations](#) on page 59

Creating and editing locations

To create or edit a location

1. In the Manager, select the **Organizations > Locations** category.
2. In the result list, select a location and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the location's main data.
4. Save the changes.






Detailed information about this topic


- [General main data for locations](#) on page 72
- [Location address information](#) on page 74
- [Configuring location networks](#) on page 75
- [Directions to location](#) on page 75
- [Functional area and risk assessment for locations](#) on page 75
- [Setting up IT operating data for departments, cost centers, and locations](#) on page 76

General main data for locations

Enter the following data for a location.

Table 17: General main data of a location

Property	Description
Location	Name of the location. Translate the given text using the  button.
Short name	Short name of the location.
Name	Additional name for the location.
Parent location	Parent of location in the hierarchy. To organize locations hierarchically, select the parent location in the menu. Leave this field empty if the location is at the top level of the location hierarchy.
Full name	Complete name of the location including parent locations. Translate the given text using the  button.
Role type	Role types for more detailed classification.
Manager	Manager responsible for the location.
2nd Manager	Assistant manager of the location.
Additional manager	Application role for a group of managers and deputies who manage this location. To create a new application role, click  . Enter the application role name and assign a parent application role.
Attestors	Applications role whose members are authorized to approve attestation cases for this location. 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.
Department	Department to which the location is primary assigned.
Cost center	Cost center to which the location is primary assigned.
Additional remarks	Text field for additional explanation.
Role approver	Application role whose members approve IT Shop requests for members of this location. To create a new application role, click  . Enter the application role name and assign a parent application role.
Role approver	Application role whose members approve IT Shop requests for

Property	Description
(IT)	members of this location. To create a new application role, click  . Enter the application role name and assign a parent application role.
Description	Text field for additional explanation.
Comment	Text field for additional explanation.
Remarks	Text field for additional explanation.
Certification status	<p>Certification status of the location. You can select the following certification statuses:</p> <ul style="list-style-type: none"> • New: The location was newly added to the One Identity Manager database. • Certified: The location main data was granted approval by the manager. • Denied: The location data was denied approval by the manager. <p>The certification status can be set depending on the result of regular attestations.</p>
Import data source	Target system or data source, from which the data set was imported.
Deactivated	Specifies whether the location is actively used. Set this option if the location is not used. This option does not have any effect on the calculation of inheritance.
Block inheritance	Specifies whether inheritance for this location can be discontinued. Set this option to discontinue inheritance within the location hierarchy.
X500 nodes	Select this option to label a location for exporting to an X500 schema.
Employees do not inherit	Specifies whether employee inheritance should be temporarily prevented for this location.
Devices do not inherit	Specifies whether device inheritance should be temporarily prevented for this location.
Workdesks do not inherit	Specifies whether workdesk inheritance should be temporarily prevented for this location.
Dynamic roles not allowed	Specifies whether a dynamic role can be created for the location.
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.
Spare date no.	Additional company-specific information. Use the Designer to

Property	Description
01 ... Spare date no. 03	customize display names, formats, and templates for the input fields.

Related topics

- [Role types for departments, cost centers, and locations on page 57](#)
- [Attestors for departments, cost centers, and locations on page 61](#)
- [Approvers and approvers \(IT\) for departments, cost centers, and locations on page 62](#)
- [Blocking inheritance using roles on page 30](#)
- [Preventing employees, devices, or workdesks from inheriting individual roles on page 31](#)
- [Creating dynamic roles for departments, cost centers, and locations on page 85](#)
- [Certifying departments, cost centers, and locations on page 90](#)

Location address information

Enter the following main data of contacting the location.

Table 18: Location's address data

Property	Description
Address	Postal address of the location.
Street	Street or road.
Building	Building
Zip code	Zip code.
City	City.
Country	Country. You require this to determine the employee's language and working hours.
State	State. You require this to determine the employee's language and working hours.
Phone	Telephone number of the location.
Quick dial	Telephone short entry (without code).
Fax	Fax number of the location.
Room	Room.

Property	Description
Comment (room)	Text field for additional explanation.

Related topics

- [Determining the language for employees](#) on page 148
- [Determining employees working hours](#) on page 149

Configuring location networks

Enter the location's network configuration data.

Table 19: Location network data

Property	Description
IP offset	IP offset of the location.
Subnet mask	Subnet mask of the location.

Directions to location



Enter another address and a description of the way to reach the location. Use the  button next to the input field to enable it and enter data. Use the  button to remove data from the list.

Table 20: Directions to location

Property	Description
Visitors address	Location address for visitors.
Travel directions	Travel directions to the location.

Functional area and risk assessment for locations

Here, you can enter values to classify a location for analyzing the risk of a location in the context of identity audit.

Table 21: Main data of a location's functional area

Property	Description
Functional area	Location's function area. This data is required for location's risk assessment.
Risk index (calculated)	A risk index is calculated for the location risk assessment based on assigned company resources. This field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Transparency index	Specifies how well you can trace location assignments. Use the slider to enter a value between 0 and 1 . 0 : no transparency 1 : full transparency
Max. number of rule violations	Number of rule violations allowed in this location. The value can be evaluated when compliance rules are checked. For more information, see the <i>One Identity Manager Compliance Rules Administration Guide</i> . NOTE: This property is only available if the Compliance Rules Module is installed.
Turnover for this unit	Turnover for this location.
Earnings for this unit	Earnings for this location.

Related topics

- [Functional areas for departments, cost centers, and locations](#) on page 59

Setting up IT operating data for departments, cost centers, and locations

To create user accounts with the **Full managed** manage level, the required IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, or cost centers. An employee is assigned a primary location, primary department, or primary cost center. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

You can also specify IT operating data directly for a specific account definition.

Example:

Normally, each employee in department A obtains a default user account in the domain A. In addition, certain employees in department A obtain administrative user accounts in the domain A.

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain A. In the IT operating data mapping rule for the account definitions A and B, specify the **Department** property in order to determine the valid IT operating data.

Specify the effective IT operating data of department A for the domain A. This IT operating data is used for standard user accounts. In addition, for department A, specify the effective IT operating data of account definition B. This IT operating data is used for administrative user accounts.

For more information, see the *One Identity Manager Target System Base Module Administration Guide*.

To define IT operating data

1. In the Manager, select the **Organizations > <role class>** category.
2. Select the role in the result list.
3. Select the **Edit IT operating data** task.
4. Click **Add** and enter the following data.
 - **Effects on:** Specify an IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.

To specify an application scope

- a. Click ➔ next to the field.
 - b. Under **Table**, select the table that maps the target system for select the TSBAccountDef table or an account definition.
 - c. Select the specific target system or account definition under **Effects on**.
 - d. Click **OK**.
- **Column:** Select the user account property for which the value is set.

In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.
 - **Value:** Enter a fixed value to assign to the user account's property.

5. Save the changes.

IT operating data for target systems

The IT operating data necessary in the One Identity Manager default configuration for automatically creating or changing employee user accounts and mailboxes in the target

system is itemized in the following table.

NOTE: IT operating data is dependent on the target system and is contained in One Identity Manager modules. The data is not available until the modules are installed.

Table 22: Target system dependent IT operating data

Target system type	IT operating data
Active Directory	Container Home server Profile server Terminal home server Terminal profile server Groups can be inherited Identity Privileged user account
Microsoft Exchange	Mailbox database
LDAP	Container Groups can be inherited Identity Privileged user account
Domino	Server Certificate Template for mail file Identity
SharePoint	Authentication mode Groups can be inherited Roles can be inherited Identity Privileged user account
SharePoint Online	Groups can be inherited Roles can be inherited Privileged user account. Authentication mode
Custom target systems	Container (per target system) Groups can be inherited

Target system type	IT operating data
	Identity Privileged user account
Azure Active Directory	Groups can be inherited Administrator roles can be inherited Subscriptions can be inherited Disabled service plans can be inherited Identity Privileged user account Change password at next login
Cloud target system	Container (per target system) Groups can be inherited Identity Privileged user account
Unix-based target system	Login shell Groups can be inherited Identity Privileged user account
Oracle E-Business Suite	Identity Groups can be inherited Privileged user account.
SAP R/3	Identity Groups can be inherited Roles can be inherited Profiles can be inherited Structural profiles can be inherited Privileged user account.
Exchange Online	Groups can be inherited
Privileged Account Management	Authentication provider Groups can be inherited Identity Privileged user account
Google Workspace	Organization

Target system type	IT operating data
	Groups can be inherited
	Products and SKUs can be inherited
	Admin roles assignments can be inherited
	Identity
	Privileged user account.
	Change password at next login
OneLogin	Roles can be inherited
	Identity
	Privileged user account.
	Licensing state
	OneLogin group

Modify IT operating data

If IT operating data changes, you must transfer the changes to the existing user accounts. To do this, templates must be rerun on the affected columns. Before you can run the templates, you can check what effect a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the One Identity Manager database in the case of each affected column in each affected database.

Prerequisites

- The IT operating data of a department, a cost center, or a location have been changed.
- OR -
- The default values in the IT operating data template were modified for an account definition.

NOTE: If the assignment of an employee to a primary department, cost center, or to a primary location changes, the templates are automatically run.

To run the template

1. In the Manager, select the **<target system type> > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Run templates** task.

This displays a list of all user accounts that were created with the selected account definition and whose properties were changed by modifying the IT operating data. That means:

- **Old value:** Value of the object property before changing the IT operating data.
 - **New value:** Value of the object property after changing the IT operating data.
 - **Selection:** Specifies whether the new value is copied to the user account.
4. Mark all the object properties in the **selection** column that will be given the new value.
 5. Click **Apply**.

The templates are applied to all selected user accounts and properties.

Assigning employees, devices, and workdesks to departments, cost centers, and locations


Assign employees, devices, and workdesks to departments, cost centers, and locations. Employees, devices, and workdesks can obtain their company resources through these organizations.

To add employees, devices, and workdesks to a hierarchical role

1. In the Manager, select the **Organizations > <role class>** category.
2. Select the role in the result list.
3. Select the appropriate task.
 - **Assign employees**
 - **Assign devices**
 - **Assign workdesks**
4. In the **Add assignments** pane, assign objects.

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

To remove an assignment

- Select the object and double-click .
5. Save the changes.

TIP: Use dynamic roles to assign employees, devices, and workdesks to departments, cost centers, and locations automatically.

Related topics

- [Preparing hierarchical roles for company resource assignments on page 24](#)
- [Assigning company resources to departments, cost centers, and locations on page 82](#)
- [Creating dynamic roles for departments, cost centers, and locations on page 85](#)
- [Assigning employees to departments, cost centers, and locations on page 138](#)
- [Assigning devices to departments, cost centers, and locations on page 168](#)
- [Assigning workdesks to departments, cost centers, and locations on page 176](#)

Assigning company resources to departments, cost centers, and locations

The default method of assigning employees, devices, and workdesks is indirect assignment. This allocates an employee, a device or a workdesk to departments, cost centers, or locations. The total of assigned company resources for an employee, a device or workdesk is calculated from their position within the hierarchy, the direction of inheritance and the company resources assigned to these roles.

Indirect assignment is divided into:

- Secondary assignment

You make a secondary assignment by classifying an employee, a device, or a workdesk within a role hierarchy. Secondary assignment is the default method for assigning and inheriting company resources through roles.

IMPORTANT: You use role classes to specify whether a secondary assignment of company resources is possible.

If an employee, device or a workdesk fulfills the requirements of a dynamic role, the object is added dynamically to the corresponding company structure and can obtain company resources through it.

- Primary assignment

You make a primary assignment using a department, cost center, or location foreign key reference in employee, device and workdesk objects. Primary assignment inheritance can be enable through configuration parameters.

You must assign company resources to departments, cost centers, or locations so that employees, devices, and workdesks can inherit company resources. The following table shows the possible company resources assignments.

NOTE: Company resources are defined in the One Identity Manager modules and are not available until the modules are installed.

Table 23: Possible company resource assignments

Company resource	Available in Module
Resources	always
Account definitions	Target System Base Module
Groups of custom target systems	Target System Base Module
System entitlements of custom target systems	Target System Base Module
Active Directory groups	Active Directory Module
SharePoint groups	SharePoint Module
SharePoint roles	SharePoint Module
LDAP groups	LDAP Module
Notes groups	Domino Module
SAP groups	SAP R/3 User Management module Module
SAP profiles	SAP R/3 User Management module Module
SAP roles	SAP R/3 User Management module Module
SAP parameters	SAP R/3 User Management module Module
Structural profiles	SAP R/3 Structural Profiles Add-on Module
BI analysis authorizations	SAP R/3 Analysis Authorizations Add-on Module
E-Business Suite permissions	Oracle E-Business Suite Module
System roles	System Roles Module
Subscribable reports	Report Subscription Module
Software	Software Management Module
Azure Active Directory groups	Azure Active Directory Module
Azure Active Directory administrator roles	Azure Active Directory Module
Azure Active Directory subscriptions	Azure Active Directory Module
Disabled Azure Active Directory service plans	Azure Active Directory Module
Unix groups	Unix Based Target Systems Module
Cloud groups	Cloud Systems Management Module
Cloud system entitlements	Cloud Systems Management Module


Company resource	Available in Module
PAM user groups	Privileged Account Governance Module
Google Workspace groups	Google Workspace Module
Google Workspace products and SKUs	Google Workspace Module
SharePoint Online groups	SharePoint Online Module
SharePoint Online roles	SharePoint Online Module
OneLogin roles	OneLogin Module

To add company resources to a hierarchical role

1. In the Manager, select the **Organizations > <role class>** category.
2. Select the role in the result list.
3. Select the task to assign the corresponding company resource.
4. 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 .
5. Save the changes.

Detailed information about this topic

- [Basic principles for assigning company resources](#) on page 15
- [Preparing hierarchical roles for company resource assignments](#) on page 24
- [Permitting assignments of employees, devices, workdesks, and company resources to roles](#) on page 29

Related topics

- [Possible assignments of company resources through roles](#) on page 25
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 81
- [Dynamic roles](#) on page 35

Creating dynamic roles for departments, cost centers, and locations

Use this task to define dynamic roles for single departments, cost centers or location. This allows you to specify memberships in these roles.

NOTE: **Create dynamic role** is only set for departments, cost centers, and locations, which do not have **Dynamic roles not allowed** set.

To create a dynamic role

1. In the Manager, select the **Organizations > <role class>** category.
2. Select the role in the result list.
3. Select the **Create dynamic role** task.
4. Enter the required main data.
5. Save the changes.

To edit a dynamic role

1. In the Manager, select the **Organizations > <Role class> > Dynamic roles** category.
2. Select the role in the result list.
3. Open the role's overview form.
4. Select **Dynamic roles** and click on the dynamic role.
5. Select the **Change main data** task.
6. Edit the dynamic role's main data.
7. Save the changes.

Related topics

- [Dynamic roles](#) on page 35
- [Creating and editing dynamic roles](#) on page 36
- [General main data for departments](#) on page 63
- [General main data for cost centers](#) on page 68
- [General main data for locations](#) on page 72

Dynamic roles with incorrectly excluded employees

In the Manager, you can obtain an overview of all the dynamic roles with conflicting entries in the exclude list. This means that for at least one item in the list the following applies:

- The dynamic role condition does not apply.
For example, this might occur if the dynamic role condition was changed after a person was entered in the exclude list.
- OR -
- The excluded person is also assigned to the role in another way
such as through inheritance or direct assignment.

Check these entries and correct the assignments.

To check conflicting entries of departments, locations, or cost centers in the exclusion list

1. In the Manager, select the **Organizations > Troubleshooting > Dynamic roles with potentially incorrect excluded employees** category.
2. Select the dynamic role in the result list.
3. Select the **Exclude employees** task.

In the exclusion list you can see which employees are affected by the given conditions.

Related topics

- [Main data of exclude lists for dynamic roles](#) on page 49
- [Removing employees from the exclusion list](#) on page 48
- [Creating dynamic roles for departments, cost centers, and locations](#) on page 85

Assign organizations

Use this task to map the relationships of a department, cost center or a location to other roles. This task has the same effect as assigning a department, cost center, or location on the role main data form. The assignment is entered in the respective foreign key column in the base table.

To assign a cost center or location to departments

1. In the Manager, select the **Organizations > Cost centers** or the **Organizations > Locations** category.
2. Select the role in the result list.
3. Select the **Assign organizations** task.
4. Select the **Departments** tab.
5. In the **Add assignments** pane, assign departments.
The selected role is primarily assigned to all departments as a cost center or location.
6. Save the changes.

To assign a department or a location to cost centers

1. In the Manager, select the **Organizations > Departments** or the **Organizations > Locations** category.
2. Select the role in the result list.
3. Select the **Assign organizations** task.
4. Select the **Cost centers** tab.
5. In the **Add assignments** pane, assign cost centers.
The selected role is primarily assigned to all cost centers as a department or location.
6. Save the changes.

To assign a department or a cost center to locations

1. In the Manager, select the **Organizations > Departments** or the **Organizations > cost centers** category.
2. Select the role in the result list.
3. Select the **Assign organizations** task.
4. Select the **Locations** tab.
5. In the **Add assignments** pane, assign locations.
The selected role is primarily assigned to all locations as a department or cost center.
6. Save the changes.

Specifying inheritance exclusion for departments, cost centers, and locations

You can define conflicting roles to prevent employees, devices, or workdesks from being assigned to several roles at the same time and from obtaining mutually exclusive company

resources through these roles. At the same time, specify which departments, cost centers, and locations are mutually exclusive. This means you may not assign these roles to one and the same employee (device, workdesk).

NOTE: Only roles, which are defined directly as conflicting roles cannot be assigned to the same employee (device, workdesk). Definitions made on parent or child roles do not affect the assignment.

To configure inheritance exclusion

- In the Designer, set the **QER | Structures | ExcludeStructures** configuration parameter and compile the database.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not 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*.

To define inheritance exclusion for a departments

1. In the Manager, select the **Organizations > Departments** category.
2. Select the department in the result list.
3. Select **Edit conflicting departments**.
4. In the **Add assignments** pane, assign departments that are mutually exclusive to the selected department.

- OR -

In the **Remove assignments** pane, remove the departments that are no longer mutually exclusive.

5. Save the changes.

To define inheritance exclusion for a cost center

1. In the Manager, select the **Organizations > Cost centers** category.
2. Select the cost center in the result list.
3. Select **Edit conflicting cost centers**.
4. In the **Add assignments** pane, assign cost centers that are mutually exclusive to the selected cost center.

- OR -

In the **Remove assignments** pane, remove the cost centers that are no longer mutually exclusive.

5. Save the changes.

To define inheritance exclusion for a cost center

1. In the Manager, select the **Organizations > Locations** category.
2. Select the location in the result list.

3. Select **Edit conflicting locations**.
4. In the **Add assignments** pane, assign locations that are mutually exclusive to the selected location.
 - OR -
 - In the **Remove assignments** pane, remove the locations that are no longer mutually exclusive.
5. Save the changes.

Detailed information about this topic

- [Inheritance exclusion: Specifying conflicting roles](#) on page 33

Assigning extended properties to departments, cost centers, and locations


You can assign extended properties to departments, cost centers, and locations. 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 set extended properties

1. In the Manager, select the **Organizations > <role class>** category.
2. Select the role in the result list.
3. Select **Assign extended properties**.
4. 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 .
5. Save the changes.

Related topics

- [Setting up extended properties](#) on page 202

Certifying departments, cost centers, and locations

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

The certification status of departments, cost centers, and locations can be set manually or by regular attestation. To set certification status by attesting, configure the attestation policies accordingly.

To manually change the certification status of a department, cost center, or location

1. In the Manager, edit the main data of the department, cost center, and location.
2. In the **Certification status** field, enter the required value.
3. Save the changes.

To change the certification status of departments, cost centers, or locations by attestation

1. In the Manager, select the **Attestation > Attestation policies** category.
2. In the result list, select the attestation policy whose attestation runs will adjust the certification status.
3. If the certification status is to change to **Certified** when attestation is approved, enable the **Set certification status to "Certified"**.
4. If the certification status is to be changed to **Denied** when attestation is denied, enable **Set certification status to "Denied"**.
5. Save the changes.

One Identity Manager provides default procedures for managers to quickly attest and certify the main data of newly added departments, cost centers, and locations in the One Identity Manager database. Attestation is performed only for organizations with the **New** certification status. If the attestation is approved, the certificate status of the attested organization is set to **Certified** and otherwise, to **Denied**. If attestation was granted approval, it disables the **Employees do not inherit** option.

NOTE: If the attestation was denied, only the certification status changes. Other behavioral changes, for example in the inheritance calculation, are not associated with this and can be implemented on a custom basis.

This function is only available if the Target System Base Module is installed. For more information about certifying new roles and organizations, see the *One Identity Manager Attestation Administration Guide*.

Detailed information about this topic

- [Creating and editing departments](#) on page 63
- [Creating and editing cost centers](#) on page 67

- [Creating and editing locations](#) on page 71

Reports about departments, cost centers, and locations

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 departments, cost centers, and locations.

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

Table 24: Reports about departments, cost centers, and locations

Report	Description
Overview of all assignments	This report finds all the roles in which employees from the selected department, cost center, or location are also members.
Data quality of department members (cost center members)	This report evaluates the data quality of employee data records. It takes all employees in the department or cost center into account.
Show historical memberships	This report lists all members of the selected department, cost center, or location and the duration of their membership.
Employees per department	This report contains the number of employee per department. The primary and secondary assignments to organizations are taken into account. You can find this report in the Manager in the My One Identity Manager category.
Employees per cost center	This report contains the number of employee per cost center. The primary and secondary assignments to organizations are taken into account. You can find this report in the Manager in the My One Identity Manager category.
Employees per location	This report contains the number of employee per location. The primary and secondary assignments to organizations are taken into account. You can find this report in the Manager in the My One Identity Manager category.

Related topics

- [Analyzing role memberships and employee assignments](#) on page 145

Employee administration

The main component of One Identity Manager maps employees with their main data and all available company resources. IT resources, such as devices, software, and access permissions in various target systems, qualify as company resources. Resources such as mobile telephones, company cars, or keys can be mapped to employees, as well.

Employees obtain company resources according to their function and their position with the company structure. Company structures, such as departments, cost centers, and location, are also mapped in One Identity Manager. As are employee memberships in these company structures. Once company resources are assigned to the company structures, they are inherited by all the members. This way, employees automatically be supplied with all the necessary company resources.

If you manage access permissions on all One Identity Manager tools using the application role, you obtain all of the information about current access permissions and employee responsibilities with One Identity Manager.

One Identity Manager components for managing employees are available when the **QER | Person** configuration parameter is set.

- In the Designer, check if the configuration parameter is set. If not, set the configuration parameter.

Detailed information about this topic

- [Employee's central user account](#) on page 99
- [Employee's default email address](#) on page 100
- [Employee's central password](#) on page 101
- [Mapping multiple employee identities](#) on page 102
- [Password policies for employees](#) on page 105
- [Creating and editing employees](#) on page 118
- [Disabling and deleting employees](#) on page 128
- [Deleting all employee related data](#) on page 131
- [Limited access to One Identity Manager](#) on page 131
- [Assigning company resources to employees](#) on page 133
- [Displaying the origin of employees' roles and entitlements](#) on page 143

- [Analyzing role memberships and employee assignments](#) on page 145
- [Employee reports](#) on page 151
- [Configuration parameters for managing employees](#) on page 211

One Identity Manager users for employee administration

Following users are used for employee administration.

Table 25: Users

Users	Tasks
Employee administrators	<p>Employee administrators must be assigned to the Identity Management Employees Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Can edit main data for all employees • Assign managers to employees. • Can assign company resources to employees. • Check and authorize employee main data. • Create and edit risk index functions. • Edit password policies for employee passwords • Delete employee's security keys (WebAuthn) • Can see everyone's requests, attestations, and delegations and edit delegations in the Web Portal.
Employee managers	<p>The Base roles Employee managers application role is automatically assigned to a user if the user is a manager or supervisor of employees, departments, locations, cost centers, business roles, or IT Shops.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Can edit main data for the objects they are responsible for and assign company resources to them. • Can edit new employees added in the Web Portal and edit the main data of their staff. • Can add their staff members to the IT Shop. • Can view their staff compliance rule violations in the Web Portal. • Can create delegations for their staff in Web Portal.

Users	Tasks
	<ul style="list-style-type: none"> • Can see and edit their staff delegations in Web Portal. <p>Members of this application role are determined through a dynamic role.</p>
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> • 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. • Create and configure password policies as required.

Basic data for employee main data

The following basic data is required for managing employees.

- Configuration parameter

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for different configuration parameters. Check the configuration parameters and modify them as necessary to suit your requirements.

Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.
- Business Partners

When external employees are entered into the system, a company must be named.
- Mail templates

The login data for new user accounts in a target system can be sent to a specified person by email. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages.
- Password policy

An employee's central password is formed from the target system specific user accounts by respective configuration. The **Employee central password policy** defines the settings for the (Person.CentralPassword) central password.


Detailed information about this topic

- [Creating and editing business partners for external employees](#) on page 95
- [Mail templates for notifications about employees](#) on page 96
- [Password policies for employees](#) on page 105
- [Configuration parameters for managing employees](#) on page 211

Creating and editing business partners for external employees

To manage external employees you require information about the business partner. Enter data for the external company.

To create or edit a business partner

1. In the Manager, select the **Employees > Basic configuration data > Business partners** category.
2. In the result list, select a company 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 26: 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.

Property	Description
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 27: 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.

Mail templates for notifications about employees

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 **Attestation > Basic configuration data > Mail templates > Predefined** category.

Related topics

- [Creating and editing mail definitions for employees](#) on page 97
- [Base object for mail templates about employees](#) on page 98
- [Editing mail templates for employees](#) on page 98

Creating and editing mail definitions for employees

For more information about creating and editing mail template, see the *One Identity Manager Operational Guide*.

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.

To create a new mail definition

1. In the Manager, select the **Employees > Basic configuration data > Mail templates** category.
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** menu.
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 **Employees > Basic configuration data > Mail templates** category.
1. Select a mail template in the result list and run the **Change main data** task.
2. In the **Mail definition** menu, select the language for the mail definition.
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.
3. Edit the mail subject line and the body text.
4. Save the changes.

Related topics

- [Base object for mail templates about employees](#) on page 98

Base object for mail templates about employees

Entering a base object in a mail template is only required if properties of the base object are referenced in the mail definition.

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, see the *One Identity Manager Configuration Guide*.

Related topics


- [Creating and editing mail definitions for employees](#) on page 97
- [Editing mail templates for employees](#) on page 98

Editing mail templates for employees

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.

To create and edit mail templates

1. In the Manager, select the **Employees > Basic configuration data > Mail templates** category.
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.


To copy a mail template

1. In the Manager, select the **Employees > Basic configuration data > Mail templates** category.
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**.

To display a mail template preview

1. In the Manager, select the **Employees > Basic configuration data > Mail templates** category.
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**.

To delete a mail template

1. In the Manager, select the **Employees > Basic configuration data > Mail templates** category.
2. Select the template in the result list.
3. Click  in the result list.
4. Confirm the security prompt with **Yes**.

Related topics

- [Creating and editing mail definitions for employees](#) on page 97

Employee's central user account

Table 28: Configuration parameter for forming the central user accounts

Configuration parameter	Meaning
QER Person CentralAccountGlobalUnique	Specifies how the central user account is mapped. If this configuration parameter is set, the central user account for an employee is formed uniquely in relation to the central user accounts of all employees and the user

Configuration parameter	Meaning
	account names of all permitted target systems. If the configuration parameter is not set, it is only formed uniquely related to the central user accounts of all employees.

The employee's central user account is used to form the user account login name in the active system. The central user account is still used for logging into the One Identity Manager tools. In One Identity Manager default installation, the central user account is made up of the first and the last name of the employee. If only one of these is known, then it is used for the central user account. One Identity Manager checks to see if a central user account with that value already exists. If this is the case, an incremental number is added to the end of the value.

Table 29: Example of forming of central user accounts

First name	Last name	Central user account
Jo		JO
	User1	J
Jo	User1	JOU
Jo	User2	JOU1

Employee's default email address

The employee's default email address is displayed on the mailboxes in the activated target system. In the One Identity Manager default installation, the default email address is formed from the employee's central user account and the default mail domain of the active target system.

The default mail domain is determined using the **QER | Person | DefaultMailDomain** configuration parameter.

- In the Designer, set the configuration parameter and enter the default mail domain name as a value.

Related topics

- [Employee's central user account](#) on page 99

Employee's central password

An employee's central password can be used for logging into the target systems and for logging in to One Identity Manager. Depending on the configuration, an employee's central password is replicated to their user accounts and their system user password.

- To publish the change in an employee's central user password to all existing user accounts of the employee, check in the Designer if the **QER | Person | UseCentralPassword** configuration parameter is set. If not, set the configuration parameter.
- To copy an employee's central password to their system user password for logging in, in the Designer, check if the **QER | Person | UseCentralPassword | SyncToSystemPassword** configuration parameter is set. If not, set the configuration parameter.
- If an employee's system user account must be unlocked if the central password is given, in the Designer, check if the **QER | Person | UseCentralPassword | SyncToSystemPassword | UnlockByCentralPassword** configuration parameter is set. If not, set the configuration parameter.

NOTE:

- The **Employee central password policy** password policy is applied to an employee's central password. Ensure that the password policy does not violate the target system's specific password policies.
- Use the **QER | Person | UseCentralPassword | CheckAllPolicies** configuration parameter to specify whether the employee's central password is tested against all the target system's password policies in which the employee has user accounts. This test is only carried out in the Password Reset Portal.
- An employee's central password is published to a user account only if the user account's target system is synchronized by the One Identity Manager.
- If a target system is read-only, an employee's central password is not propagated to user accounts in that target system.
- An employee's central password is not replicated to privileged user accounts of the employee.
- If a password cannot be changed due to an error, the employee receives a corresponding email notification.
- To replicate an employee's central password to a password column of a customer-specific user account table, in the Designer, define a ViewAddOn for the QERVPersonCentralPwdColumn view. The database view returns the password column of the user account tables. The user account table must have a reference to the employee (UID_Person) and a XMarkedForDeletion column. For more information about modifying the One Identity Manager schema, see the *One Identity Manager Configuration Guide*.
- If you want to map additional user-specific features, overwrite the QER_Publish_CentralPassword script. For more information about editing scripts, see the *One*

Identity Manager Configuration Guide.

- The central password, the system user password, and the user account passwords can be changed by using the Password Reset Portal. For more information, see the *One Identity Manager Web Designer Web Portal User Guide* and the *One Identity Manager Web Application Configuration Guide*.

Related topics

- [Miscellaneous employee main data](#) on page 125
- [Password policies for employees](#) on page 105
- [Displaying locked employees and system users](#) on page 118

Mapping multiple employee identities

Table 30: Configuration parameter for representing multiple identities

Configuration parameter	Effect when set
Person MasterIdentity UseMasterForAuthentication	<p>Specifies whether the main identity should be used to log in to One Identity Manager tools using an employee-linked authentication module.</p> <p>If this parameter is set, the main identity is used for employee-linked authentication. If this parameter is set, the subidentity is used for employee-linked authentication.</p> <p>For more information about One Identity Manager authentication modules and about editing system users, see the <i>One Identity Manager Authorization and Authentication Guide</i>.</p>

Under certain circumstances, it may be necessary for employees to have different identities for their work – for example, identities that result from different contracts at different branches. These identities can differ in their affiliation to departments, or cost centers, or in their access permissions for example. External employees at different locations can also be used and represented with different identities in the system. You can define a main identity and a subidentity for an employee in One Identity Manager to represent each of the identities and to group them at a central location.

In target systems, different types of user accounts are available to provide the employees with different permissions. An employee can have different identities to use multiple user accounts with different types. In order to improve the assignment of authorizations to the target systems, the sub-identities of the employees are split into different identity types. This classification corresponds to the user account types.

Main identity

- A main identity represents a real person.
- A main identity can be assigned user accounts and permissions in One Identity Manager and it can place requests in the IT Shop.
- The employee main data of a main identity is shown in One Identity Manager.
- A main identity can have several subidentities.

Subidentity

- A subidentity is a virtual employee.
- A subidentity can be assigned user accounts and permissions in One Identity Manager and it can place requests in the IT Shop.
- A subidentity is always assigned to a main identity.
- Employee main data of a subidentity is displayed in One Identity Manager. This can be copied from the main identity data using the appropriate templates.
- Enter a main identity for the subidentity using **Main identity** on the employee's main data form.

TIP: If an employee works with several identities, but only one of these is currently known in the One Identity Manager, then you should:

- Create a main identity for this employee
- Assign the identity known until now as a subidentity
- Create new subidentities for the additional identities

In this way, it is possible to test the employee's permitted permissions per subidentity or per main identity including all subidentities in the bounds of an identity audit.

Related topics

- [Employee identity types](#) on page 103

Employee identity types

To differentiate the different identities of an employee, use the following identity types.

Table 31: Identity types

Value	Description
Primary identity	Employee's default identity. The employee has a default user account.
Organizational identity	Virtual employee (subidentity) for mapping different roles to an employee in the organization. The sub-identity has a user account of

Value	Description
	the Organizational identity type. Also enter a main identity.
Personalized admin identity	Virtual employee (subidentity) that belongs to a user account of the Personalized administrator identity type. Also enter a main identity.
Sponsored identity	Pseudo employee associated with a user account of the Sponsored identity type. Assign a manager to the employee.
Shared identity	Pseudo employee associated with an administrative user account of the Shared identity type. Assign a manager to the employee.
Service identity	Pseudo employee associated with a user account of the Service identity type. Assign a manager to the employee.
Machine identity	Pseudo employee for mapping machine identities.

The primary identity, the organizational identity, and the personal admin identity are different identities under which the same actual employee can run their different tasks within the company.

Employees with a personal admin identity or an organizational identity are set up as sub-identities. These subidentities are then linked to user accounts, enabling you to assign the required permissions to the different user accounts.

The sponsored identity, the shared identity, and the service identity represent pseudo employees that are used to provide the linked user accounts with permissions in the respective target systems. The classification of pseudo employees to hierarchical roles or as customers in the IT Shop enables the assignment of permissions to the user accounts. Requests in the IT Shop can be triggered only by the manager of these pseudo employees. When evaluating reports, attestations, or compliance checks, check whether pseudo employees need to be considered separately.

Related topics

- [Miscellaneous employee main data](#) on page 125
- [Mapping multiple employee identities](#) on page 102

Password policies for employees

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password policies apply not only when the user enters a password but also when random passwords are generated.

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

Detailed information about this topic

- [Predefined password policies](#) on page 105
- [Applying employee password policies](#) on page 106
- [Creating password policies for employees](#) on page 109
- [Custom scripts for password requirements](#) on page 113
- [Defining the excluded list for passwords](#) on page 116
- [Checking employee passwords](#) on page 116
- [Generating passwords for testing employees](#) on page 117
- [Informing employees about expiring passwords](#) on page 117

Predefined password policies

You can customize predefined password policies to meet your own requirements if necessary.

Password for logging in to One Identity Manager

The **One Identity Manager password policy** is applied for logging in to One Identity Manager. This password policy defines the settings for the system user passwords (DialogUser.Password and Person.DialogUserPassword) as well as the passcode for a one time log in on the Web Portal (Person.Passcode).

NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The **Employee central password policy** defines the settings for the (Person.CentralPassword) central password. Members of the **Identity Management | Employees | Administrators** application role can adjust this password policy.

IMPORTANT: Ensure that the **Employee central password policy** does not violate the target system-specific requirements for passwords.

Password policies for user accounts

Predefined password policies are provided, which you can apply to the user account password columns of the user accounts. You can define password policies for user accounts for various base objects, for example, for account definitions, manage levels, or target systems.

For more information about password policies for user accounts, see the administration guides of the target systems.

Related topics

- [Employee's central password](#) on page 101

Applying employee password policies

The **One Identity Manager password policy** and **Employee central password policy** are predefined password policies for employees' central passwords.

You can assign custom password policies to employees' password columns. You can also assign the password policies to departments, cost centers, locations, or business roles, and therefore apply password policies depending on the employees' organizational classification.

Which password policy is applied to a person is determined in the following order:

1. Password policy of the employee's primary business role
2. Password policy of the employee's primary department
3. Password policy of the employee's primary location
4. Password policy of the employee's primary cost center
5. General password policy for employee passwords
6. The **One Identity Manager password policy** (default policy)

Related topics

- [Predefined password policies](#) on page 105
- [Changing the password policy for password columns](#) on page 107
- [Assigning password policies to departments, cost centers, locations, and business roles](#) on page 107

Changing the password policy for password columns

If you do not want to apply the predefined password policy to the password column of employees, change the password policy assignment to the base object in the Manager.

To change a password policy's assignment

1. In the Manager, select the **Employees > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.
4. In the **Assignments** pane, select the assignment you want to change.
5. From the **Password Policies** menu, select the new password policy you want to apply.
6. Save the changes.

Assigning password policies to departments, cost centers, locations, and business roles

You can assign the password policies for forming an employee's system user password, the passcode, and an employee's central password to departments, cost centers, locations, and business roles.

NOTE: If you want to use the assignment of a password policy through company structures, you need to decide whether to use either departments, cost centers, locations, or business roles. Otherwise, performance problems may occur when determining the valid password policy. A large number of hierarchy levels could also lead to performance problems when determining the password policy to apply.

To reassign a password policy

1. In the Manager, select the **Employees > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.
4. Click **Add** in **Assignments** and enter the following data.

- **Apply to:** Application scope of the password policy.

To specify an application scope

1. Click ➔ next to the field.
2. Under **Table**, select the table that contains the basic objects. You have the following options:
 - Departments (Department table)
 - Business roles (Org table)

NOTE: This table is only available if the Business Roles Module is installed.
 - Locations (Locality table)
 - Cost centers (Profitcenter table)
3. Under **Apply to**, select the specific department, cost center, location, or business role.
4. Click **OK**.
- **Password column:** Name of the password column. You have the following options:
 - **Employees - central password** (Person table, CentralPassword column)
 - **Employees - password** (Person table, DialogUserPassword column)
 - **Employees - passcode** (Person table, Passcode column)
- **Password policy:** Name of the password policy to use.
5. Save the changes.

Editing password policies for employees

Predefined password policies are supplied with the default installation that you can use or customize if required.

To edit a password policy

1. In the Manager, select the **Employees > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Edit the password policy's main data.
5. Save the changes.

Detailed information about this topic

- [General main data for password policies](#) on page 109
- [Password policy settings](#) on page 110
- [Character classes for passwords](#) on page 111
- [Custom scripts for password requirements](#) on page 113

Creating password policies for employees

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

To create a password policy

1. In the Manager, select the **Employees > Basic configuration data > Password policies** category.
2. On the main data form, enter the main data of the password policy.
3. Save the changes.




Detailed information about this topic

- [General main data for password policies](#) on page 109
- [Password policy settings](#) on page 110
- [Character classes for passwords](#) on page 111
- [Custom scripts for password requirements](#) on page 113

General main data for password policies

Enter the following main data of a password policy.

Table 32: main data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the  button.
Description	Text field for additional explanation. Translate the given text using the  button.
Error Message	Custom error message generated if the policy is not fulfilled. Translate the given text using the  button.

Property	Meaning
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. This option cannot be changed. NOTE: The One Identity Manager password policy is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

Password policy settings

Define the following settings for a password policy on the **Password** tab.

Table 33: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated. NOTE: The initial password is not used as an employee's system user password. You can implement this behavior by customizing if required.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is 0 , no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is 256 .
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is 0 , the number of failed logins is not taken into account. This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has exceeded the maximum number of failed logins, the employee or system user will not be able to log in to One Identity Manager.

Property	Meaning
	You can use the Password Reset Portal to reset the passwords of employees and system users who have been blocked. For more information, see the <i>One Identity Manager Web Designer Web Portal User Guide</i> .
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is 0 , then the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of 5 is entered, the user's last five passwords are stored. If the value is 0 , then no passwords are stored in the password history.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value 0 means that the password strength is not tested. The values 1 , 2 , 3 and 4 specify the required complexity of the password. The value 1 represents the lowest requirements in terms of password strength. The value 4 requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the Contains name properties for password check option is set. In the Designer, adjust this option in the column definition. For more information, see the <i>One Identity Manager Configuration Guide</i> .

Character classes for passwords

Use the **Character classes** tab to specify which characters are permitted for a password.

Table 34: Character classes for passwords

Property	Meaning
Required number of character classes	<p>Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for Min. number letters, Min. number lowercase, Min. number uppercase, Min. number digits, and Min. number special characters.</p> <p>That means:</p> <ul style="list-style-type: none"> Value 0: All character class rules must be fulfilled.

Property	Meaning
	<ul style="list-style-type: none"> Value >0: Minimum number of character class rules that must be fulfilled. At most, the value can be the number of rules with a value >0. <p> NOTE: Generated passwords are not tested for this.</p>
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special characters	List of special characters that are not permitted.
Do not generate lowercase letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.

Property	Meaning
Do not generate digits	Specifies whether a generated password can contain digits. This setting only applies when passwords are generated.
Do not generate special characters	Specifies whether a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

Custom scripts for password requirements

You can implement custom scripts for testing and generating passwords if the password requirements cannot be mapped with the existing settings options. Scripts are applied in addition to the other settings.

Detailed information about this topic

- [Checking passwords with a script](#) on page 113
- [Generating passwords with a script](#) on page 115

Checking passwords with a script

You can implement a script if additional policies need to be used for checking a password that cannot be mapped with the available settings.

Syntax of check scripts

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
```

With parameters:

policy = password policy object

spwd = password to check

TIP: To use a base object, take the Entity property of the PasswordPolicy class.

Example: Script that checks a password

A password cannot start with ? or ! . The password cannot start with three identical characters. The script checks a given password for validity.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or
'!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in
password")#)
        End If
    End If
End Sub
```

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
 - a. In the Manager, select the **Employees > Basic configuration data > Password policies** category.
 - b. In the result list, select the password policy.
 - c. Select the **Change main data** task.
 - d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
 - e. Save the changes.

Related topics

- [Generating passwords with a script](#) on page 115

Generating passwords with a script

You can implement a generating script if additional policies need to be used for generating a random password, which cannot be mapped with the available settings.

Syntax for generating script

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

With parameters:

policy = password policy object

spwd = generated password

TIP: To use a base object, take the Entity property of the PasswordPolicy class.

Example: Script that generates a password

In random passwords, this script replaces the invalid characters ? and ! at the beginning of a password with _.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

```
    Dim pwd = spwd.ToInsecureArray()
```

```
    ' replace invalid characters at first position
```

```
    If pwd.Length>0
```

```
        If pwd(0)="?" Or pwd(0)="!"
```

```
            spwd.SetAt(0, CChar("_"))
```

```
        End If
```

```
    End If
```

```
End Sub
```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
 - a. In the Manager, select the **Employees > Basic configuration data > Password policies** category.
 - b. In the result list, select the password policy.
 - c. Select the **Change main data** task.

- d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.
- e. Save the changes.

Related topics

- [Checking passwords with a script](#) on page 113

Defining the excluded list for passwords

You can add words to a list of restricted terms to prohibit them from being used in passwords.

| NOTE: The restricted list applies globally to all password policies.

To add a term to the restricted list

1. In the Designer, select the **Base data > Security settings > Password policies** category.
2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude from the list.
3. Save the changes.

Checking employee passwords

When you verify a password, all the password policy settings, custom scripts, and the restricted passwords are taken into account.

To verify if a password conforms to the password policy

1. In the Manager, select the **Employees > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Select the table and object to be tested in **Base object for test**.
6. Enter a password in **Enter password to test**.

A display next to the password shows whether it is valid or not.

Generating passwords for testing employees

When you generate a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To generate a password that conforms to the password policy

1. In the Manager, select the **Employees > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Click **Generate**.

This generates and displays a password.

Informing employees about expiring passwords

There are different ways to inform users that their password is going to expire:

- Users are alerted about their password expiring when they log in to One Identity Manager and can change their password if necessary.
- For employee-based authentication modules, the system sends reminder notifications in relation to expiring passwords as of seven days in advance of the password expiry date.
 - You can adjust the time in days in the **Common | Authentication | DialogUserPasswordReminder** configuration parameter. Edit the configuration parameter in the Designer.
 - The notifications are triggered in accordance with the **Reminder system user password expires** schedule and use the **Employee - system user password expires** mail template. You can adjust the schedule and mail template in the Designer if required.

For more information about One Identity Manager authentication modules and about editing system users, see the *One Identity Manager Authorization and Authentication Guide*.

Displaying locked employees and system users

If a user has exceeded the maximum number of failed logins, the employee or system user will not be able to log in to One Identity Manager.

- Locked employees are displayed in the Manager in the **Employees > Locked employees** category. An additional message referring to the locked login is also displayed on the overview form for an employee.
- Locked system users are displayed in the Designer in the **Permissions > System users > Locked system users** category. An additional message referring to the locked login is also displayed on the overview form for a system user.

You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. This unlocks the employees and system users again. For more information, see the *One Identity Manager Web Designer Web Portal User Guide* and the *One Identity Manager Web Application Configuration Guide*.

Related topics

- [Employee's central password](#) on page 101

Creating and editing employees

In One Identity Manager, you can manage main data of company employees as well as external employees. Because the described main data is the same for internal and external employees, the **Employee** term is used in the following description.

In the Manager, enter employee main data in the **Employees** category. Employees are filters by different criteria in this category.

- **Employees:** All activated and temporarily deactivated employees.
- **Inactive employees:** All permanently deactivated employees.
- **Locked employees:** All employees who are locked due to incorrect password input.
- **Certification:** All employees by certification status.
- **Data source:** All employees by import data source.
- **Identity:** All employees according to their identity type.

To create or edit employees

1. In the Manager, select the **Employees > Employees** category.
2. Select an employee in the result list and run the **Change main data** task.
 - OR –

Click  in the result list.

This opens the main data form for an employee.

3. Edit the employee's main data.
4. Save the changes.

Ensure you fill out all compulsory fields when you edit the main data. Certain main data is inherited by the employee user account through templates.

NOTE: Employee properties loaded from a target system can only be edited to a limited degree in One Identity Manager. Certain properties are locked because this target system is the primary system. The source from which the employee main data is imported determines which properties are locked.

Detailed information about this topic

- [General employee main data](#) on page 119
- [Organizational employee main data](#) on page 122
- [Address data for employees](#) on page 124
- [Miscellaneous employee main data](#) on page 125


General employee main data

Enter the following general main data of an employee. This data applies to personal and job-related employee data.

Table 35: General main data

Property	Description
First name	Employee's first name.
Last name	Employee's last name.
Middle name	Second middle name.
Form of address	Employee's form of address. This is automatically set depending on gender.
Title	Employee's title.
Surname prefix	Employee's surname prefix, for example du , or von .
Preferred name	Employee's preferred name.
Initials	Employee's initials. These are automatically taken from first and last names.

Property	Description
Gender	Employee's gender.
Date of birth	Employee's date of birth.
Name at birth	Employee's name at date.
Job description	Description of employee's job within your company.
Generational affix	Affix, for example Senior or Junior .
Language	Language used for sending email notifications to the employee. This setting is also used for Web Portal's display.
Language for value formatting	Language used to display values, for example, date, time, or number formats. The setting is taken into account when email notifications are sent to the employee. This setting is also used for Web Portal's display.
Sub-organization	Note about sub-organizations to which the Employee belongs.
Permanently disabled	<p>Specifies whether the employee is currently employed by the company. If this option is set, the employee has left the company. All privileges as One Identity Manager user are removed.</p> <p>NOTE: Employees who are permanently deactivated can no longer log in to One Identity Manager.</p>
Certification status	<p>Specifies whether the employee main data was approved by the employee's manager. Certification status is set through certification procedures. The following certification status are permitted:</p> <ul style="list-style-type: none"> • New: The employee was newly added to the One Identity Manager database. • Certified: The employee main data has been approved by the manager. • Denied: The employee main data was not approved by the manager. The employee is permanently disabled.
VIP	Labels the employee as important.
Security risk	<p>Specifies whether the employee is considered a risk for the company. Resource inheritance can be prevented for employees who are classified as security risks. Configure the behavior in the resource properties. Permissions inheritance can be prevented for employees who are classified as security risks. The user accounts of the employee can be blocked. Configure this in the account definition properties. For more information about account definitions, see the <i>One Identity Manager Target System Base Module Administration Guide</i>.</p>

Property	Description
	<p>NOTE: Employees who are classified as a security risk are no longer be able to log in to One Identity Manager. To allow login, set the QER Person AllowLoginWithSecurityIncident configuration parameter.</p>
No inheritance	<p>Specifies whether the employee inherits company resources through roles. If this option is set, the employee cannot inherit. Company resources the employee receives through IT Shop requests are not assigned either. Direct assignments remain intact.</p> <p>If the configuration parameter QER Attestation UserApproval is set, this option is set depending on the option Disabled permanently. If the employee is permanently disabled, the option No inheritance is set through a formatting rule.</p>
External	<p>Specifies whether the employee is employed internally or externally by your company. If this option is set, the employee is external. External employees are excluded from automatic account definition assignment in the default version of One Identity Manager.</p>
Employee type	<p>More accurate classification of the employee taking their contractual relationship with the company into account. Permitted values are Employee, Apprentice, Contractor, Consultant, Partner, Customer, Other.</p>
Contact email address	<p>Email address to which the registration link is sent when a new user account is created using the Self-Registration Web Portal.</p>
Company	<p>Enter a company. Use the  next to the field to add a new company.</p>
Workdesk	<p>Employee's workdesk.</p>
Risk index (calculated)	<p>A risk index is calculated to evaluate the risk of an employee based on their permissions. An employee's risk index is determined from the risk indexes of their user accounts. This field is only visible if the QER CalculateRiskIndex configuration parameter is set. For more information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p>
Description	<p>Text field for additional explanation.</p>
Comment	<p>Text field for additional explanation.</p>
Spare field no. 01 ... Spare field no. 10	<p>Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.</p>

Related topics

- [Changing the certification status of employees](#) on page 132
- [Permanently deactivating employees](#) on page 129

- [Blocking inheritance using roles](#) on page 30
- [Calculation of assignments](#) on page 22
- [Creating and editing business partners for external employees](#) on page 95
- [Creating and editing workdesks](#) on page 171
- [Main data for resources](#) on page 190

Organizational employee main data

Enter the following general main data of an organization.

Table 36: Organizational main data

Property	Description
Personnel number	Employee's personnel number.
Primary department	<p>Department to which the employee is primary assigned. The employee can obtain company resources through this assignment when One Identity Manager is configured respectively.</p> <p>Furthermore, IT operating data for user accounts and mailboxes can be determined through the department.</p>
Primary cost center	<p>Cost center to which the employee is primarily assigned. The employee can obtain company resources through this assignment when One Identity Manager is configured respectively.</p> <p>Furthermore, IT operating data for user accounts and mailboxes can be determined through the cost center.</p>
Primary business roles	<p>Business role to which the employee is assigned. The employee can obtain company resources through this assignment when One Identity Manager is configured respectively.</p> <p>Furthermore, IT operating data for user accounts and mailboxes can be determined through the business role.</p> <p>NOTE: This property is available if the Business Roles Module is installed.</p>
Security identification	Security code for the employee for, for example, access permission.
User account creation date	Date on which to create the user account in the target system. This date should be earlier than the entry date. Use custom processes to automatically create user accounts in One Identity Manager on this date.
Entry date	Date the employee started at the company. This is filled with the current date when the employee is added.

Property	Description
End date	Date the employee started at the company. Enter an end date for the employee to lock their user account at a specific point in time. The end date is checked regularly by the schedule Lock accounts of employees that have left the company . When the end date arrives, the employee is blocked.
Company member	Additional information about the employee's affiliation.
Temporarily disabled	Specifies whether the employee is temporarily absent from the company. If this option is set, enter the time period for the temporary absence. NOTE: Employees who are temporarily deactivated can no longer log in to One Identity Manager.
Temporarily disabled from	Date from which the employee and associated user accounts are disabled.
Temporarily disabled until	Date until which the employee and associated user accounts are disabled. A Enable temporarily disabled accounts schedule is implemented that monitors the end date of the temporary deactivation. When this date is reached the employee and their user accounts are re-enabled.
Last working day	Enter the date of the last working day if, for example, an employee leaves the company on a specific day but has access to their data until this date. NOTE: The date of the last working day is copied to the employee's user accounts as the expiration date. This overwrites the existing account expiration date.
Manager	An employee's manager can assume several tasks in One Identity Manager such as: <ul style="list-style-type: none"> • Edit employee main data of their staff • Certify employee main data of their staff • Attest company resources assigned to their staff • Approve request for their staff in the IT Shop Employee cannot be assigned as their own manager.
Sponsor	When a new employee is added through the Web Portal, you can make additional notes like the manager or sponsor.


Related topics

- [Preparing hierarchical roles for company resource assignments](#) on page 24
- [Permanently deactivating employees](#) on page 129
- [Temporarily deactivating employees](#) on page 128

Address data for employees

Enter the following data for an employee, which describes the employee's location in the company.

Table 37: Address data

Property	Description
Primary location	Location to which the employee is primarily assigned. The employee can obtain company resources through this assignment if One Identity Manager is configured respectively. Furthermore, IT operating data for user accounts and mailboxes can be determined through the location.
Phone	Employee's telephone number.
Mobile phone	Employee's mobile number.
Fax	Employee's fax number.
Display in phone book	Specifies whether the employee are shown in the telephone book.
Street	Street or road.
Building	Building
Office mailbox	Office mailbox.
Zip code	Zip code.
City	City.
Country	Country. You require this to determine the employee's language and working hours. This data is usually stored with the employee's location or department data. You can also enter it directly by the employee. This setting is also used for Web Portal's display.
State	State. You require this to determine the employee's language and working hours. This data is usually stored with the employee's location or department data. You can also enter it directly in the employee's data.
Floor	Floor.
Room	Room.
Image	You can import a picture of the employee into the database. To do this, use the  button next to the picture box to browse the image to be displayed.

Related topics

- [Preparing hierarchical roles for company resource assignments](#) on page 24
- [Determining the language for employees](#) on page 148
- [Determining employees working hours](#) on page 149

Miscellaneous employee main data

Enter the following general main data of an employee. This data applies to the target system login, identities, One Identity Manager login data, and employee import data.

Table 38: Miscellaneous main data

Property	Description
Central user account	One Identity Manager user identifier. In One Identity Manager default installation, the central user account is made up of the first and the last name of the employee. An employee's central user account affects the composition of user accounts in each target system. The central user account is still used for logging into the One Identity Manager tools.
Central SAP user account	Name used to form the user account name in the SAP R/3 target system. In the One Identity Manager default installation, the central user account is made up of the first and the last name of the employee. NOTE: This property is only available if the SAP R/3 User Management module Module is installed.
E-Business Suite user account	Name used to form the user account name in the Oracle E-Business Suite target system. In the One Identity Manager default installation, the E-Business Suite user account is formed from the employee's central user account. NOTE: This property is only available if the Oracle E-Business Suite Module is installed.
E-Business Suite ID	Unique ID for the HR employee, the AP customer, the AP supplier or the AR parties in the Oracle E-Business Suite. NOTE: This property is only available if the Oracle E-Business Suite Module is installed.
E-Business Suite employee ID	Personnel number of the HR employee in the Oracle E-Business Suite. NOTE: This property is only available if the Oracle E-Business Suite Module is installed.
Central password and password confirmation	An employee's central password can be used for logging into the target systems and for logging in to One Identity Manager. Depending on the configuration, an employee's central password is replicated to their user accounts and their system user password.

Property	Description
	Use the Password Reset Portal to change the central password. For more information, see the <i>One Identity Manager Web Designer Web Portal User Guide</i> .
Decentralized identity and confirmation	Identifier of the decentralized identity to identify the employee. This identifier can be used to log in to One Identity Manager.
Default email address	Default email address for setting up the employee's mailboxes in the individual target systems. This data is absolutely necessary for automatically creating mailboxes. In the One Identity Manager default installation, the default email address is composed of the employee's central user account and the default mail domain of the active target system.
Identity	Identity type of the person.
Main identity	Allocate a main identity here if the employee is managed as a sub-identity in the One Identity Manager. A subidentity allows you to set up special cases in One Identity Manager. If an employee has several user accounts in one target system that must be assigned to different groups, create a separate subidentity for each user account with a link to the main identity.
Pseudo employee	Specifies whether the employee represents an actual employee or a pseudo employee used for connecting to administrative user accounts, for example.
Actual employee	Unique ID of the actual employee.
X500 pseudo employee	Specifies whether the employee is managed as an X500 pseudo employee in the One Identity Manager. If an employee has several X500 entries with different properties, you can also use pseudo employee here. Label the employee with the option X500 pseudo employee for the user case and configure a link to the real X500 employee.
X500 employee	Assign the X500 pseudo employee to an existing employee.
Logins	<p>Logins with which the employee can log in to the One Identity Manager administration tools. Enter the login in the form: Domain\User. This information is required if the authentication modules User account and User account (role-based) are used for logging in to One Identity Manager tools.</p> <p>For more information about One Identity Manager authentication modules, see the <i>One Identity Manager Authorization and Authentication Guide</i>.</p>
System users	System user with which the employee can log in to the One Identity

Property	Description
	<p>Manager administration tools. The login data is analyzed by the authentication module in use.</p> <p>For more information about One Identity Manager authentication modules, see the <i>One Identity Manager Authorization and Authentication Guide</i>.</p>
System user password and password confirmation	<p>Employee's system user password. Password with which the employee logs in to the One Identity Manager tools.</p> <p>Use the Password Reset Portal to change the system user password. For more information, see the <i>One Identity Manager Web Designer Web Portal User Guide</i>.</p>
User account name (mainframe)	If an employee is permitted access to the mainframe with their user account, enter the login name here.
Notebook user	Just for information.
Company car	Just for information.
Login permitted on terminal server	Specifies whether this employee is permitted to log in on the terminal server with their user account.
Remote access permitted	Specifies whether the employee can dial in to the network with their user account.
Resetting the password through the help desk is permitted.	Specifies whether the password can be reset with the help of password help desk staff. If this option is set, password help desk staff in the Operations Support Web Portal can reset the employee's password.
Help desk employee	<p>Specifies whether the employee can handle help desk calls. For more information about the help desk, see <i>One Identity Manager Help Desk Module User Guide</i>.</p> <p> NOTE: This option is only available if the Helpdesk Module is installed.</p>
Import data source	Target system or data source respectively, from which the employee was imported. This property is also set by scripts for automatically assigning employees to user accounts.
Distinguished name	Distinguished name of the imported employee. This property should be set by the import.
Canonical name	Fully qualified name of the imported employee. This property should be set by the import.

Related topics

- [Employee's central user account](#) on page 99
- [Employee's central password](#) on page 101
- [Employee's default email address](#) on page 100
- [Mapping multiple employee identities](#) on page 102
- [Employee identity types](#) on page 103

Disabling and deleting employees

How employees are handled, particularly in the case of permanent or partial withdrawal of an employee, varies between individual companies. There are companies that never delete employees, and only disable them when they leave the company.

Detailed information about this topic

- [Temporarily deactivating employees](#) on page 128
- [Permanently deactivating employees](#) on page 129
- [Reactivate permanently deactivated employees](#) on page 130
- [Deferred deletion of employees](#) on page 130

Temporarily deactivating employees

NOTE: Employees who are temporarily deactivated can no longer log in to One Identity Manager.

The employee has temporarily left the company and is expected to return at a predefined date. The desired course of action could be to disable the user account and remove all group memberships. Or the user accounts could be deleted and reestablished with the employee's return, even if it is with a new system identification number (SID).

Temporary disabling of an employee is triggered by:

- The **Temporary disabled** option
- The start and end date for deactivation (**Temporary disabled from** and **Temporary disabled until**)

NOTE:

- Configure the **Lock accounts of employees that have left the company** schedule in the Designer. This schedule checks the start date for disabling and sets the **Temporarily disabled** option when it is reached.

- In the Designer, configure the **Enable temporarily disabled accounts** schedule. This schedule monitors the end date of the disabled period and enables the employee with their user accounts when the date expires. Employee's user accounts that were disabled before the period of temporary absence are also re-enabled once the period has expired.

Related topics

- [Permanently deactivating employees](#) on page 129
- [Deferred deletion of employees](#) on page 130

Permanently deactivating employees

NOTE: Employees who are permanently deactivated can no longer log in to One Identity Manager.

Employees can be deactivated permanently when, for example, they leave the company. It might be necessary, to remove access to this employee's entitlements in connected target systems and their company resources.

Effects of permanent deactivating an identity are:

- The employee cannot be assigned to employees as a manager.
- The employee cannot be assigned to roles as a supervisor.
- The employee cannot be assigned to attestation policies as an owner.
- There is no inheritance of company resources through roles, if the additional **No inheritance** option is set for an employee.
- Employee user accounts are locked or deleted and then removed from group memberships.

Trigger permanent deactivation through:

- The **Deactivate employee permanently** task

This task ensures that the **Permanently deactivates** option is enabled and the leaving date and last working day are set to the current date.

- The leaving date is reached

NOTE:

- In the Designer, check the **Lock accounts of employees that have left the company** schedule. This schedule regularly checks the leaving date and sets the **Permanently deactivated** option on reaching the date.
- The **Re-enable employee** task ensures that the employee is re-enabled.
- The **Denied** certification status

If an employee's certification status is set to **Denied** manually or as a result of attestation, the employee is immediately permanently deactivated. When the

employee's certification status is changed to **Certified**, the employee is activated again.

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

Related topics

- [Temporarily deactivating employees](#) on page 128
- [Deferred deletion of employees](#) on page 130
- [Reactivate permanently deactivated employees](#) on page 130
- [Changing the certification status of employees](#) on page 132

Reactivate permanently deactivated employees

Employees who are permanently deactivated can be re-enabled if they were not disabled by certification.

To reactivate an employee

1. In the Manager, select the **Employees > Inactive employees** category.
2. Select the employee in the result list.
3. Select the **Reactivate employee** task.
4. Confirm the security prompt with **Yes** if the employee should be enabled.

On the main data form for the employee, the **Permanently deactivated** option is not set. The end date and last working day are deleted assuming the dates are past.

5. Save the changes.

Related topics

- [Permanently deactivating employees](#) on page 129

Deferred deletion of employees

When an employee is deleted, the system checks whether user accounts and company resources are still assigned to the employee or whether requests are open in the IT Shop. The employee is marked for deletion and therefore locked out of further processing.

By default, employees are finally deleted from the database after 30 days. During this period it is possible to re-enable the employee. A restore is not possible once deferred deletion has expired.

In the Designer, you can set an alternative delay on the Person table. For more information on configuring the deferred deletion, refer to the *One Identity Manager Configuration Guide*.

Before an employee can finally be deleted from the One Identity Manager database, you need to delete all company resource assignments and close all requests. You can do this manually or implement custom processes to do it.

All the user accounts linked to an employee can be deleted by default by One Identity Manager once this employee has been deleted. If no more company resources are assigned, the employee is finally deleted.

Related topics

- [Temporarily deactivating employees](#) on page 128
- [Permanently deactivating employees](#) on page 129

Deleting all employee related data

A procedure called QER_PPersonDelete_GDPR is provided to support the special process for deleting employee related data, which implements the General Data Protection Regulation (GDPR) of the European Union. You can use this procedure to delete all data relating to an employee from the One Identity Manager database. For certain dependencies, processes that are handled by the One Identity Manager Service are created by the procedure.

NOTE: While this procedure is running, the database does not allow any triggers. Therefore, it is recommended to only run the procedure in maintenance periods.

You can run the procedure in any program suitable for running SQL queries.

Calling syntax:

```
exec QER_PPersonDelete_GDPR ' <employee UID from the Person table, UID_Person column>'
```

NOTE: Personal data may be subject to further regulations such as legal retention periods. Personal data from the One Identity Manager History Database is not automatically deleted by default because of this. It is recommended to operate One Identity Manager History Databases that correspond to the report periods. After a specified reporting period has expired, you can set up a new One Identity Manager History Database. You set up custom processes for deleting personal data.

Limited access to One Identity Manager

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

Users who only have temporary or limited access to the One Identity Manager can log in through the Web Portal. This functionality can be used, for example, if external employees,

such as contract workers, should be provided with temporary access to the One Identity Manager. These employee can log in to the Web Portal as new workers. New employee objects are added for them in the One Identity Manager database.

If you make use of this functionality, take note of the following:

- In One Identity Manager, an employee with the following properties is created:
 - **Certification status:** New
 - **Permanently deactivated:** Set
 - **No inheritance:** Set
- If the **QER | Attestation | UserApproval** configuration parameter is set, the new employee is attested automatically.
- To assign company resources to the employee or to ensure permissions in One Identity Manager, implement custom processes.

For more information about attestation, see the *One Identity Manager Attestation Administration Guide*.

Related topics

- [Changing the certification status of employees](#) on page 132

Changing the certification status of employees

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

Employee's certification status is set by default through certification and recertification procedures. For more information, see the *One Identity Manager Attestation Administration Guide*.

You can manually change an employee's certification status if it is necessary to do so outside the regular recertification schedule.

Prerequisite

- The **QER | Attestation | UserApproval** configuration parameter is set.

To change an employee's certification status manually

1. To change the certification status of an active employee, in the Manager, select the **Employees > Employees.** category.

- OR -

To change the certification status of a permanently deactivated employee, in the Manager, select the **Employees > Inactive employees** category.

2. Select the employee in the result list.
3. Select the **Change certification status** task.
4. Select the certification status you want from the **Certification status** menu.
5. Click **OK** to accept the changes.

The new certification status for the employee is displayed on the form.

NOTE: The **Permanently deactivated** option is updated depending on the certification status. If an employee's certification status is set to **Denied** manually or as a result of attestation, the employee is immediately deactivated permanently. If the employee's certification status is changed to **Certified**, the employee is activated again.

Related topics

- [Limited access to One Identity Manager](#) on page 131
- [Permanently deactivating employees](#) on page 129

Assigning company resources to employees

One Identity Manager uses different assignment types to assign company resources.

- Indirect assignment

In the case of indirect assignment of company resources, employees, devices, and workdesks are arranged in departments, cost centers, locations, business roles, or application roles. The total of assigned company resources for an employee, device, or workdesk is calculated from the position within the hierarchies, the direction of inheritance (top-down or bottom-up) and the company resources assigned to these roles. In the Indirect assignment methods a difference between primary and secondary assignment is taken into account.

- Direct assignment

Direct assignment of company resources results from the assignment of a company resource to an employee, device, or workdesk, for example. Direct assignment of company resources makes it easier to react to special requirements.

- Assignment by dynamic roles

Assignment through dynamic roles is a special case of indirect assignment. Dynamic roles are used to specify role memberships dynamically. Employees, devices, and workdesks are not permanently assigned to a role, just when they fulfill certain conditions. A check is performed regularly to assess which employees, devices, or workdesks fulfill these conditions. This means the role memberships change dynamically. For example, company resources can be assigned dynamically to all

employees in a department in this way; if an employee leaves the department they immediately lose the resources assigned to them.

- Assigning through IT Shop requests

Assignment through the IT Shop is a special case of indirect assignment. Add employees to a shop as customers so that company resources can be assigned through IT Shop requests. All company resources assigned as product to this shop can be requested by the customers. Requested company resources are assigned to the employees after approval is granted. Role memberships can be requested through the IT Shop as well as company resources.

The following table shows the possible company resources assignments to employees.

NOTE: Company resources are defined in the One Identity Manager modules and are not available until the modules are installed.

Table 39: Possible assignments of company resources to employees

Company Resource	Direct assignment permitted	Indirect assignment permitted	Comment
Resources	+	+	
System roles	+	+	
Subscribable reports	+	+	
Software	+	+	
Account definitions	+	+	
Groups of custom target systems	-	+	All the employee's user accounts of the custom target systems, which permit group inheritance, are assigned to the groups.
System entitlements of custom target systems	-	+	All the employee's custom target system user accounts, which permit system entitlement inheritance, are assigned to the custom target system system entitlements.
Active Directory groups	-	+	All the employee's Active Directory user accounts and Active Directory contacts of the employee, which permit group inheritance, are assigned to the Active Directory groups.
SharePoint groups	-	+	All the employee's SharePoint user accounts, which permit group

Company Resource	Direct assignment permitted	Indirect assignment permitted	Comment
			inheritance, are assigned to the SharePoint groups.
SharePoint roles	-	+	All the employee's SharePoint user accounts, which permit group inheritance, are assigned to the SharePoint roles.
LDAP groups	-	+	All the employee's LDAP user accounts, which permit group inheritance, are assigned to the LDAP groups.
Notes groups	-	+	All the employee's Notes user accounts, which permit group inheritance, are assigned to the Notes groups.
SAP groups	+	+	All the employee's SAP user accounts, which are in the same SAP client and for which group inheritance is permitted, are assigned to the SAP groups.
SAP profiles	+	+	All the employee's SAP user accounts, which are in the same SAP client and for which group inheritance is permitted, are assigned to the SAP profiles.
SAP roles	+	+	All the employee's SAP user accounts, which are in the same SAP client and for which group inheritance is permitted, are assigned to the SAP roles.
Structural profiles	-	+	All the employee's SAP user accounts, which are in the same SAP client and for which group inheritance is permitted, are assigned to the structural profiles.
BI analysis authorizations	-	+	All the employee's BI user accounts, which permit group inheritance, are assigned to the BI analysis authorizations.

Company Resource	Direct assignment permitted	Indirect assignment permitted	Comment
E-Business Suite permissions	-	+	All the employee's E-Business Suite user accounts, which are in the same E-Business Suite system and for which group inheritance is permitted, are assigned to the E-Business Suite groups.
Azure Active Directory groups	-	+	All the employee's Azure Active Directory user accounts, which permit group inheritance, are assigned to the Azure Active Directory groups.
Azure Active Directory administrator roles	-	+	All the employee's Azure Active Directory user accounts, which permit group inheritance, are assigned to the Azure Active Directory administrator roles.
Azure Active Directory subscriptions	-	+	All the employee's Azure Active Directory user accounts, which permit group inheritance, are assigned to the Azure Active Directory subscriptions.
Disabled Azure Active Directory service plans	-	+	All the employee's Azure Active Directory user accounts, which permit group inheritance, are assigned to the disabled Azure Active Directory service plans.
Unix groups	-	+	All the employee's Unix user accounts, which permit group inheritance, are assigned to the Unix groups.
PAM user groups	-	+	All the employee's PAM user accounts, which permit group inheritance, are assigned to the PAM user groups.
SharePoint Online groups	-	+	All the employee's SharePoint Online user accounts, which permit group inheritance, are assigned to the SharePoint Online groups.
SharePoint Online roles	-	+	All the employee's SharePoint Online user accounts, which permit group inheritance, are assigned to the SharePoint Online roles.

Company Resource	Direct assignment permitted	Indirect assignment permitted	Comment
Google Workspace products and SKUs	-	+	All the employee's Google Workspace user accounts, which permit group inheritance, are assigned to the Google Workspace products and SKUs.
Google Workspace groups	-	+	All the employee's Google Workspace user accounts, which permit group inheritance, are assigned to the Google Workspace groups.
Cloud groups	-	+	All the employee's cloud user accounts, which permit group inheritance, are assigned to the cloud groups.
Cloud system entitlements	-	+	All the employee's cloud user accounts, which permit system entitlement inheritance, are assigned to the cloud system entitlements.

Detailed information about this topic

- [Basic principles for assigning company resources](#) on page 15
- [Permitting assignments of employees, devices, workdesks, and company resources to roles](#) on page 29

Related topics

- [Possible assignments of company resources through roles](#) on page 25
- [Assigning employees to departments, cost centers, and locations](#) on page 138
- [Assigning employees to business roles](#) on page 139
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 81
- [Assigning company resources to departments, cost centers, and locations](#) on page 82
- [Dynamic roles](#) on page 35

Assigning employees to departments, cost centers, and locations


Assign the employee to departments, cost centers, and locations so employees obtain their company resources through these organizations. To assign company resources to departments, cost centers, and locations, use the appropriate organization tasks.

To assign an employee to departments, cost centers, and locations (secondary assignment; default method)

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign organizations** task.
4. 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 .
5. Save the changes.

To assign an employee to departments, cost centers, and locations (primary assignment)

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Change main data** task.
4. Adjust the following main data on the **Organizational** tab.
 - Primary department
 - Primary cost center
 - Primary location
5. Save the changes.

Related topics

- [Assigning company resources to employees](#) on page 133
- [Assigning company resources to departments, cost centers, and locations](#) on page 82
- [Dynamic roles](#) on page 35
- [Adding employees to IT Shop custom nodes](#) on page 139

- [Assigning employees to business roles](#) on page 139
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 81

Assigning employees to business roles

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


Assign employees to business roles so that employees obtain their company resources through these business roles. To assign company resources to business roles use the corresponding business role tasks. For more information about working with business roles, see the *One Identity Manager Business Roles Administration Guide*.

To assign an employee to business roles (secondary assignment; default method)

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign business roles** task.
4. 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 .
5. Save the changes.

To assign an employee to business roles (primary assignment)

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Change main data** task.
4. On the **Organizational** tab, enter the primary business role.
5. Save the changes.

Related topics

- [Assigning company resources to employees](#) on page 133

Adding employees to IT Shop custom nodes

When employees are added to a custom node they are entitled to make IT Shop requests. Access permissions to the IT Shop and the assignments allocated to them through product

requests in the IT Shop are displayed on the employee's overview. For more information, see the *One Identity Manager IT Shop Administration Guide*.

To add an employee to the IT Shop

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign IT Shop memberships** task.
4. In the **Add assignments** pane, assign custom nodes.

- OR -

In the **Remove assignments** pane, remove the custom nodes.

5. Save the changes.

Assigning application roles to employees

For more information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Assigned employees obtain all the permissions of the permission group to which the application role (or a parent application role) is assigned. In addition, employees obtain the company resources assigned to the application role.

If there are no employees directly assigned to an application role, the employees of the parent application role inherit the permissions.


NOTE: The application roles for **Base roles | Everyone (Change)**, **Base roles | Everyone (Lookup)**, **Base roles | Employee Managers**, and **Base roles | Birth-right Assignments** are automatically assigned to employees. Do not make any manually assignments to these application roles.

To assign application to an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign One Identity Manager application roles** task.
4. In the **Add assignments** pane, assign the application roles.

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

To remove an assignment

- Select the application role and double-click .
5. Save the changes.

Assigning resources directly to employees

Resources can be assigned directly or indirectly to employees. Indirect assignment is carried out by allocating employees and resources in company structures, like departments, cost centers, locations, or business roles.


To react quickly to special requests, you can assign resources directly to an employee.

To assign resources directly to an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee to whom the resources will be assigned, from the result list.
3. Select the **Assign resources** task.
4. In the **Add assignments** pane, assign resources.

TIP: In **Remove assignments**, you can remove assigned resources.

To remove an assignment

- Select the resource and double-click .
5. Save the changes.

Related topics

- [Assigning resources directly to employees](#) on page 193
- [Managing resources](#) on page 187

Assigning software directly to employees

NOTE: This function is only available if the Software Management Module is installed.

You can assign software directly or indirectly to employees. Indirect assignment is carried out by allocating employees and software in company structures, like departments, cost centers, locations, or business roles. For more information about working with software, see the *One Identity Manager Software Management Administration Guide*.

To react quickly to special requests, you can assign software directly to an employee.

To assign software directly to an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee to whom the software will be assigned, from the result list.
3. Select the **Assign software** task.
4. In the **Add assignments** pane, assign software.

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

To remove an assignment

- Select the software and double-click ✓.
5. Save the changes.

Assigning system roles directly to employees

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

System roles can be assigned directly or indirectly to employees. Indirect assignment is carried out by allocating the employees and system roles in company structures, such as departments, cost centers, locations, or business roles. For more information about working with system roles, see the *One Identity Manager System Roles Administration Guide*.

To react quickly to special requests, you can assign system roles directly to an employee.

To assign system roles directly to an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click ✓.
5. Save the changes.

Assigning subscribable reports directly to employees

NOTE: This function is only available if the Report Subscription Module is installed.

You can assign subscribable reports directly or indirectly to employees. Indirect assignment is carried out by assigning the employee and subscribable report to company structures, like departments, cost centers, locations, or business roles. For more information about report subscriptions, see the *One Identity Manager Report Subscriptions Administration Guide*.


In order to react quickly to special requests, you can also assign subscribable reports directly to employees.

To assign user accounts to an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign subscribable reports** task.
4. In the **Add assignments** pane, assign reports.

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

To remove an assignment

- Select the report and double-click .
5. Save the changes.

Displaying the origin of employees' roles and entitlements

The **Show entitlements origin** report allows you to determine which entitlements an employee owns and where they come from. You can establish whether the employee obtained an entitlements directly or indirectly. For example, in the case of an indirect assignment, you can determine whether the entitlement resulted from a department memberships or a request,

You can also use the report to discover which departments, cost centers, locations, and business roles are assigned to an employee and how the membership evolved.

To use the origin report

- In the Designer, set the **SysConfig | Display | SourceDetective** configuration parameter and compile the database.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not 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*.

To display the origin of an employee's entitlements

1. In the Manager, select the **Employees > Employees** category.
2. Select an employee in the result list and run the **Show entitlements origin** report.
3. Under **Assigned objects**, you will see the employee's entitlements, departments, cost centers, locations, and business roles. Select an entry by double-clicking on it to view more details.
4. The **Origin** area displays the details for the selected entry in a hierarchical structure. You can see whether the assignment was a direct assignment, dynamic assignment, or a request.

- You can use the **Details** button to switch to the dynamic role or to the request.
- Double-click on some of the entries in the detail view to go to the object.
- Choose the **Inspect** button for further information about the assignment of authorizations.

Example: Report on an entitlement's origin

The **Show entitlements origin** report establishes that Jo User1 is assigned to the Active Directory "Finance" group.

The screenshot shows the One Identity Manager interface. On the left, a list of employees is displayed, with 'Harris, Clara (CLARA.H)' selected. On the right, the 'Assigned objects' table lists various objects and their types. The 'Origin' section at the bottom shows the 'Finance' group and its assignments, including 'Active Directory user accounts: <Harris Clara>' and 'Active Directory user accounts: assignments to groups: <Harris Clara - Finance>'.

The report answers several questions.

Question Why does Jo User1 have the Active Directory group?

Answer Jo User1 owns an Active Directory user account and this user account is assigned to the "Finance" group.

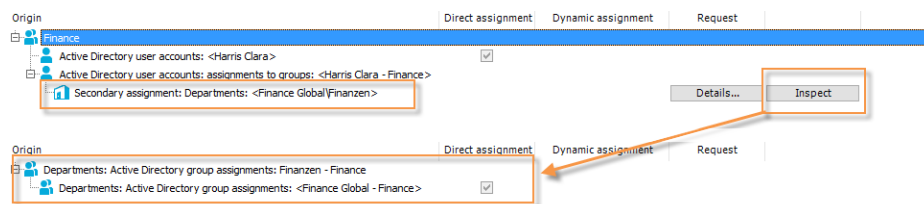
The screenshot shows the 'Origin' section of the One Identity Manager interface. It displays the 'Finance' group and its assignments, including 'Active Directory user accounts: <Harris Clara>' and 'Active Directory user accounts: assignments to groups: <Harris Clara - Finance>'.

Question Why is the user account assigned to the "Finance" group?

Answer Jo User1 is assigned to the "Finance" department.

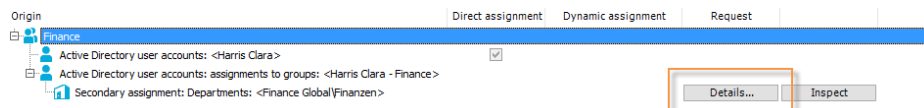
The screenshot shows the 'Origin' section of the One Identity Manager interface. It displays the 'Finance' group and its assignments, including 'Active Directory user accounts: <Harris Clara>' and 'Active Directory user accounts: assignments to groups: <Harris Clara - Finance>'.

The "Finance" department inherits from the "Global Finance" department. The "Global Finance" department is directly assigned to the "Finance" group.



Question Why is Jo User1 in the "Finance" department?

Answer There is a department membership request for Jo User1.




Analyzing role memberships and employee 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 employees who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Examples:

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

Figure 13: Toolbar of the Overview of all assignments report.



Table 40: 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.

Displaying the employees overview

Use this task to obtain an overview of the most important information about an employee.

To obtain an overview of an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Employee overview** task.

The most important information about an employee is shown on this form, including the employee's contact data, user accounts, and affiliation to company structures.

The assigned company resources and access to IT Shop structures and IT Shop requests are displayed.

The employee's responsibilities within the One Identity Manager are displayed on the form. This includes the application roles that an employee has been assigned within the One Identity Manager and the functions as department manager, cost center manager, or approver within the IT Shop.

4. Select the **Employee entitlements overview** task.

This form shows the system entitlements and all the target system groups allocated to an employee.

Displaying and deleting employees' Webauthn security keys

One Identity offers users the option to log in, simply and securely, to One Identity Manager web applications with help of (physical) security keys. These security keys support the W3C standard **WebAuthn**.

For more information about using security keys in the Web Portal, see the *One Identity Manager Web Designer Web Portal User Guide*. For more about configuring this method, see the *One Identity Manager Web Application Configuration Guide*.

As personnel administrator, you can view employees' security keys and delete them if necessary.

To display an employee's security key

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Show webauthn security keys** task.
This shows all the employee's security keys.
4. Select one of the security keys in the list to show its details.

To delete an employee's security key

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Show webauthn security keys** task.
4. Select the security in the list and click **Remove**.
5. Save the changes.

Determining the language for employees

In order for email notifications within the request process in the IT Shop or during attestation to be sent in the recipients language, the employee's language has to be determined.

- States and countries and their languages already exist in the One Identity Manager default installation. Verify and edit this information in the Designer. For more information, see the *One Identity Manager Configuration Guide*.
- Add the country and state of the primary location to the primary department, the primary cost center, the primary business role, or directly to the employee. To map special cases, you can also add the language directly to the location, department, cost center, or employee.

An employee's language is determined in the following order:

1. Language that is directly assigned to the employee.
2. Language of the employee's state.
3. Language of the employee's country.
4. Language directly assigned to the employee's location.
5. Language of the primary location's state.
6. Language of the primary location's country.
7. Language directly assigned to the employee's primary department.
8. Language of the primary department's state.
9. Language of the primary department's country.
10. Language directly assigned to the employee's primary cost center.
11. Language of the primary cost center's state.
12. Language of the primary cost center's country.
13. Language directly assigned to an employee's primary business role
14. Language of the primary business role's state.
15. Language of the primary business role's country.
16. Fallback, in case the language could not be determined with this sequence:
 - a. Language from the **Common | MailNotification | DefaultCulture** configuration parameter.
 - b. Language **en-US**.

Determining employees working hours

An employee's working hours need to be made public in order to determine the reaction times of approvers or attestors to request processes in the IT Shop or during attestation.

- States and countries and their time zones, public holidays, and standard working hours already exist in One Identity Manager. Verify and edit this information in the Designer. For more information, see the *One Identity Manager Configuration Guide*.
- The employee's location (state or country) must be determined so that the working hours can be calculated correctly. Add the country and state to the primary location, the primary department, the primary cost center, the primary business role, or directly to the employee.
- The correct working hours are subsequently calculated. The standard working hours in the country, rule for weekends and holidays, as well as different time zones and daylight-saving rules, are taken into account when the hours are calculated.

The employee's location and therefore valid working hours, are determined in the following order:

1. State that is directly assigned to the employee.
2. Country that is directly assigned to the employee.
3. State of primary location.
4. Country of primary location.
5. State of primary department.
6. Country of primary department.
7. State of primary cost center.
8. Country of primary cost center.
9. State of primary business role.
10. Country of primary business role.
11. Fallback, in case the location could not be determined with this sequence:
 - a. State or country using the secondary location, department, or cost center.
 - b. First country from all enabled countries in the database sorted by telephone number
 - c. Country entered as default in the database (DialogDatabase table, UID_ DialogCountryDefault column).
For more information, see the *One Identity Manager Configuration Guide*.
 - d. Country **USA**.

Manually assigning user accounts to employees

The overview form displays all the employee's user accounts. You should use account definitions as the default method for creating user accounts. For more information about account definitions, see the *One Identity Manager Target System Base Module Administration Guide*.

To react quickly to special requests, you can use the relevant tasks for assigning user accounts to manually assign a user account for an employee.

NOTE: The tasks for manually assigning user accounts to persons are defined in the One Identity Manager modules and are only available when the modules have been installed. For more information, see the target system guides.

Related topics

- [Displaying the employees overview](#) on page 146

Entering calls for employees

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

Enter the calls for employees through the Helpdesk Module. For more information about the help desk, see *One Identity Manager Help Desk Module User Guide*.

To enter help desk data for an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Show calls** task to display calls entered for an employee task.
4. Select the **New call** task to enter a new call.
5. Save the changes.

Assigning extended properties to employees


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 specify extended properties for a group

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign extended properties** task.
4. 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 .
5. Save the changes.

Related topics

- [Creating and editing extended properties](#) on page 204

Employee reports

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 employees.

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

Table 41: Employee reports

Report	Description
Entitlement Origins	The report shows an employee's entitlements and roles and the possible assignment methods.
Request history	<p>The report provides you with an overview of each IT Shop request made by an employee. The report is divided into approved, canceled, denied, and pending requests. You can trace when and why each product was requested, renewed, or unsubscribed.</p> <p>View completed requests by clicking on Show. In the approval history you can see the approval workflow, the results of each approval step and the approver. The Show button shows you the current approval status of pending requests.</p>
Data quality of direct reports	This report evaluates the data quality of employee data records. All employees under supervision are taken into account.
Employees	This report contains the number of employee per department. The

Report	Description
per department	primary and secondary assignments to organizations are taken into account. You can find this report in My One Identity Manager .
Employees per cost center	This report contains the number of employee per cost center. The primary and secondary assignments to organizations are taken into account. You can find this report in My One Identity Manager .
Employees per location	This report contains the number of employee per location. The primary and secondary assignments to organizations are taken into account. You can find this report in My One Identity Manager .
Data quality summary for employee records	The report contains different analyzes of data quality for all employees. You can find this report in My One Identity Manager .
Access overview at specific point-in-time	This report contains detailed information about personal and organizational data as well as an overview of the company resources that the employee owned at a specific point-in-time. This includes all assigned user accounts, system entitlements, roles, account definitions, resources, and software.
Attestation cases	<p>The report shows completed and pending attestation cases for which the person was identified as the attestor. If the employee is logged in to the Manager, they can use the report to grant or deny attestation case approval. Use Approve or Deny to grant or deny approval. Enter the reason in Approval reason and click on the Carry out approval button. If a report has been defined for the attestation instance, you can view it using the Show report button in the column.</p> <p>Use the Show attestation history task to display each step in the attestation case. This allows you to track the chronological sequence and approvals in the attestation case. The attestation history is displayed for pending and closed attestations.</p> <p> NOTE: This report is available if the Attestation Module exists.</p>
Overview with roles and user accounts	<p>The report contains detailed information about personal and organizational data as well as user accounts, roles, and entitlements currently assigned to the employee.</p> <p>You can decide whether to include dependent identities in the report.</p>
Overview with roles and user accounts (including history)	<p>The report contains detailed information about personal and organizational data as well as user accounts, roles, and entitlements currently assigned to the employee including historical data.</p> <p>Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.</p> <p>You can decide whether to include dependent identities in the report.</p>

Report	Description
	<p> NOTE: This report is available if the Target System Base Module exists.</p>
Direct reports overview	<p>The report shows all employees that report directly. This displays detailed information about personal and organizational data as well as current user accounts, roles, and entitlements.</p> <p> NOTE: This report is available if the Target System Base Module exists.</p>
Direct reports overview (including history)	<p>All employees that report directly including the history. This shows detailed information about personal and organizational data as well as current user accounts, roles, and entitlements including the historical data.</p> <p>Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.</p>
Show user accounts overview (including history)	<p>This report returns all the user accounts with their permissions including a history.</p> <p>Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.</p> <p> NOTE: This report is available if the Target System Base Module exists.</p>
User accounts of direct reports (including history)	<p>This report returns all the user accounts with their permissions including a history.</p> <p>Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.</p> <p> NOTE: This report is available if the Target System Base Module exists.</p>
Show owned system entitlements (incl. history)	<p>This report shows the system entitlements with the assigned user accounts including a history.</p> <p>Select the end date for displaying the history (Min. date). Older changes and assignments that were removed before this date, are not shown in the report.</p> <p> NOTE: This report is available if the Target System Base Module exists.</p>
Overview of employee's privileged access.	<p>The report contains detailed information about personal and organizational data as well as the employee's current privileged access.</p> <p> NOTE: This report is available if the Privileged Account Governance Module exists.</p>

Related topics

- [Displaying the origin of employees' roles and entitlements](#) on page 143
- [Analyzing role memberships and employee assignments](#) on page 145

Managing devices and workdesks

One Identity Manager offers extended device administration functionality for networks. One Identity Manager differentiates between device types, device models, and the device itself.

- Device types, such as PCs, printers, or monitors, provide the initial classification of the devices.
- Device models provide additional fine-tuning of the device types in order to obtain a more exact classification of devices.
- The actual devices as they are defined in the network are listed under devices.

Workdesks are required for assigning different devices to a workstation. The assignment of company resources can be mainly automated by assigning workdesks to business roles, departments, cost centers, locations, or dynamic roles.

To manage devices and workdesks in One Identity Manager

- In the Designer, set the **Hardware** configuration parameter and compile the database.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not 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*.

Detailed information about this topic

- [Basic data for device admin](#) on page 155
- [Creating and editing devices](#) on page 161
- [Assigning company resources to devices](#) on page 167
- [Creating and editing workdesks](#) on page 171
- [Assigning company resources to workdesks](#) on page 174
- [Asset data for devices](#) on page 181

Basic data for device admin

The following basic data is required for managing devices:

- Configuration parameter

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for different configuration parameters. Check the configuration parameters and modify them as necessary to suit your requirements.

Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.

- Device models

Device models are required to classify devices, for example, PC, server, monitor, printer types. One Identity Manager contains predefined device models.

- Information about manufacturers and suppliers

You can store manufacturers and suppliers to help with entering device models and devices, .

- Device status

Enter the possible device status for asset data about devices.

- Workdesk status

You can add a status to workdesks.

- Workdesk types

Provide workdesk types for further classification of workdesks,

Detailed information about this topic


- [Creating and editing device models](#) on page 155
- [Creating and editing business partners](#) on page 158
- [Creating and editing device statuses](#) on page 159
- [Creating and editing workdesk statuses](#) on page 160
- [Creating and editing workdesk types](#) on page 160
- [Configuration parameters for managing devices and workdesks](#) on page 214

Creating and editing device models

The prerequisite for adding devices is the definition of device models. Device models are required to classify devices, for example, PC, server, monitor, printer types. One Identity

Manager contains predefined device models. You can define more device models.

To create or edit a device model

1. In the Manager, select the **Devices & Workdesks > Basic configuration data > Device models** category.
2. In the result list, select a device model and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the device model's main data.
4. Save the changes.




Detailed information about this topic

- [General main data for device models](#) on page 156
- [Inventory data for device models](#) on page 157

General main data for device models

Enter the following general main data of a device model.

Table 42: Device model main data

Property	Description
Device model	Name of the device model.
Device type	Type of the device. During the setup of new device, the device model's device type filters the forms that are available for handling main data.
Company	Name of manufacturer. Use the  next to the field to add a new company. For more information, see Creating and editing business partners on page 158. NOTE: Only the companies that are marked as manufacturers can be selected. When a new device is added, the company named as manufacturer in the device model is used for the device.
Service item	If you assigned a service item to the device model, the usage of the device model can be booked internally. Use the  next to the field to add a new service item.
Website	Manufacturers Website. Click the  button to display the manufacturer's website in the default web browser.
Description	Text field for additional explanation.
Additional data	Text field for additional explanation.

Property	Description
PC	Specifies whether, in principle, the device can be used as a PC in the sense of workstation.
Server	Specifies whether the device is used as a server.
Local peripheral	Specifies whether this device type is a local peripheral to attach to a PC.
Deactivated	Specifies whether the device model is in use or not. NOTE: Only device models which are enabled can be assigned in One Identity Manager. If a device model is deactivated, assignment of the device model is not permitted. However, existing assignments remain intact.

Inventory data for device models

You can enter the following inventory and asset data for a device model.

NOTE: Prices are given to 2 decimal places by default. The number of decimal places to enter can be modified in the Designer. For more information, see the *One Identity Manager Configuration Guide*.

Table 43: Inventory data for a device model


Property	Description
Default supplier	Name of supplier. For more information, see Creating and editing business partners on page 158.
Employee	Employee responsible for the purchase.
Alternative device model	Alternative device model.
Warranty [months]	Standard manufacturer warranty in months.
Additional guarantee [months]	Additional manufacturer guarantee in months.
Usage [months]	Estimated period of use.
Minimum stock	Minimum level of stock in storage.
Maximum stock	Maximum level of stock in storage.
Item number	Article number at suppliers.
Request units	Measurement units for requests.
Minimum request quantity	Minimum quantity for requests.

Property	Description
Last quote date	Last quote date.
Price of last offer	Price of last offer.
Last delivery date	Last delivery date.
Price of last delivery	Price of last delivery.

Creating and editing business partners

Enter data for external companies that might be used as manufacturers, suppliers, or leasing partners.

To create or edit a business partner

1. In the Manager, select the **Devices & Workdesks > Basic configuration data > Business partners** category.
2. In the result list, select a company 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 44: 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	Customers number at supplier.

Property	Description
number	
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 45: 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.

Creating and editing device statuses

You can define the status that devices take on, for example: activated, deactivated, stored.

To create or edit a device status

1. In the Manager, select the **Devices & Workdesks > Basic configuration data > Device status** category.
2. In the result list, select a device status and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the device's main data.
4. Save the changes.

Enter the following data for a device status.


Table 46: Device status general data

Property	Description
Device status	Name of the device status.
Short description	Text field for additional explanation.
Description	Text field for additional explanation.

Creating and editing workdesk statuses

Enter the statuses that workdesks are able to have, for example, activated, deactivated, stored.

To create or edit a workdesk status

1. In the Manager, select the **Devices & Workdesks > Basic configuration data > Workdesk status** category.
2. In the result list, select a workdesk status and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the workdesk status's main data.
4. Save the changes.

Enter the following data for a workdesk status.

Table 47: Main data for a workdesk


Property	Description
Status	Workdesk status name.
Short description	Text field for additional explanation.
Description	Text field for additional explanation.

Creating and editing workdesk types

Provide workdesk types for further classification of workdesks. Enter additional device prerequisites for a workdesk.

To create or edit a workdesk type

1. In the Manager, select the **Devices & Workdesks > Basic configuration data > Workdesk type** category.

2. In the result list, select a workdesk type and run the **Change main data** task.
 - OR -
 - Click  in the result list.
3. Edit the workdesk type's main data.
4. Save the changes.

Enter the following data for a workdesk type.

Table 48: Main data for a workdesk type

Property	Description
Workdesk type	Name of the workdesk type.
Display name	Name for displaying in the One Identity Manager tools.
Short description	Text field for additional explanation.
Description	Text field for additional explanation.
Leasing fee	Leasing fee.
Floppy disk drive required	Specifies whether this workdesk type requires a floppy disk drive.
CD-ROM drive required	Specifies whether this workdesk type requires a CD-ROM drive.

Creating and editing devices

Table 49: Configuration parameter for setting up a device

Configuration parameter	Effect when set
Hardware Display CustomHardwareType	When a new device is set up with the corresponding device model, the data is displayed in a customized form.
Hardware Display CustomHardwareType MobilePhone	Add a device type that represents a mobile phone.
Hardware Display CustomHardwareType Monitor	Add a device type that represents a monitor
Hardware Display CustomHardwareType PC	Add a device type that represents a PC.
Hardware Display CustomHardwareType Printer	Add a device type that represents a printer.


Configuration parameter	Effect when set
Hardware Display CustomHardwareType Server	Add a device type that represents a server.
Hardware Display CustomHardwareType Tablet	Add a device type that represents a tablet.
Hardware Display MachineWithRPL	Data for remote booting of workstations and servers can be edited.
Hardware Workdesk WorkdeskAuto	When workstation or server is setup an associated workdesk is created automatically.

You can manage different devices with One Identity Manager, for example, workstations, servers, monitors, printers, or other devices.

To create or edit a device

1. In the Manager, select the **Devices & Workdesks > Devices** category.
2. Select one of the following nodes.
 - Personal computer
 - Server
 - Monitors
 - Printer
 - Mobile telephones
 - Tablets
 - Miscellaneous

Depending on the selected filter, the device model is specified and the corresponding form for editing the main data determined when a new device is added.

3. In the result list, select a device and run the **Change main data** task.
- OR -
Click  in the result list.
4. Edit the device's main data.
5. Save the changes.

Detailed information about this topic

- [General main data for devices](#) on page 163
- [Device networking data](#) on page 165
- [Asset data for devices](#) on page 181
- [Assigning company resources to devices](#) on page 167

General main data for devices

Enter the following general main data of a device. The main data available depends on the selected device model.

Table 50: General main data of a device

Property	Description
Asset number	Number of the asset in the bookkeeping.
Device ID	Unique device ID.
PC	Specifies whether the device is a computer.
Server	Specifies whether the device is a server.
Local peripheral	Specifies whether this is a local peripheral such as a monitor, printer, or other peripheral device.
Manufacturer	Name of manufacturer.
Device model	Name of the device model. The main data available depends on the selected device model.
Device status	Device's status.
Workdesk	The device's workdesk. This workdesk is used to assign various devices to a workstation or a server. If the Hardware Workdesk WorkdeskAuto configuration parameter is set, a workdesk bearing the same name is automatically created when a workstation or a server is set up.
Parent device	A parent device which is linked to this device.
VM Client (option)	Specifies whether this device is a virtual machine.
VM Host	Device on which a virtual machine is installed. The selection is shared if the VM client is set.
VM Host (option)	Specifies whether this device is a virtual machine host.
Phone	Telephone number.
Used by	Employee who uses this device.
Primary department	Department to which the device is primary assigned. Company resources can be inherited by a device through these primary assignments if One Identity Manager is appropriately configured.
Primary location	Location to which the device is primary assigned. Company resources can be inherited by a device through these primary assignments if One

Property	Description
	Identity Manager is appropriately configured.
Primary cost center	Cost center to which the device is primary assigned. Company resources can be inherited by a device through these primary assignments if One Identity Manager is appropriately configured.
Primary business roles	Business role to which the device is assigned. Company resources can be inherited by a device through these primary assignments if One Identity Manager is appropriately configured. NOTE: This property is available if the Business Roles Module is installed.
Investment	Investments or investment plans for the device.
Location description	Text field for additional explanation.
Description	Text field for additional explanation.
Remarks	Text field for additional explanation.
No inheritance	Specifies whether the device inherits company resources through roles. If this option is set, the employee cannot inherit. Direct assignments remain intact.
Operating system	Operating system identifier.
Operating system version	Version number of the operating system.
Service pack operating system	Service pack identifier.
Hotfix operating system	Hotfix identifier.
Carrier	Carrier contract for the device.
Serial number	Manufacturer's serial number.
MAC address	The device's MAC address.
IMEI	The device's IMEI number.
ICCID	The device's ICCID number.
BIOS version	Version of the BIOS.
Number of processors	Number of processors in the device.

Property	Description
RAM [MB]	RAM in megabytes.
1. capacity [MB]	Capacity of the first disk in megabytes
2. capacity [MB]	Capacity of the second disk in megabytes
Max. vertical resolution	Maximum vertical image resolution.
Max. horizontal resolution	Maximum horizontal image resolution.
Import data source	Target system or data source, from which the data set was imported.
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.

Related topics

- [Creating and editing device models](#) on page 155
- [Creating and editing business partners](#) on page 158
- [Creating and editing device statuses](#) on page 159
- [Asset data for devices](#) on page 181
- [Entering investments and investment plans for devices](#) on page 183
- [Creating and editing workdesks](#) on page 171
- [Basic principles for assigning company resources](#) on page 15
- [Preventing inheritance to individual employees, devices, or workdesks](#) on page 31

Device networking data

Enter the following information for the network configuration. The main data available depends on the selected device model.

Table 51: Network data

Property	Description
IP address (IPv4)	IP address in IPv4 format.

Property	Description
IP address (IPv6)	IP address in IPv6 format.
Use DHCP	Specifies whether the IP address is taken from a DHCP server. If this option is not set, enter a fixed IP address and enter the subnet mask and standard gateway.
Subnet mask	Subnet mask.
Default gateway	Default gateway.
Use WINS	Specifies whether WINS name resolution is used. If this option is set, enter the IP addresses of the preferred and the alternative WINS server.
WINS primary	IP address of the preferred WINS server.
WINS secondary	IP address of the alternative WINS server.
Range ID	To communicate with one another, all computers require a TCP/IP network with the same area ID. The area ID is used for identification when the given DNS server cannot be found. Normally, this input should be left empty.
Use DNS	Specifies whether WINS name resolution is used. If this option is set, enter the IP address of the preferred and the alternative DNS server.
DNS server	IP address of the preferred DNS server.
2. DNS server	IP address of the alternative DNS server.
3. DNS server	IP address of the alternative DNS server.
DNS name	Suffix of DNS domain the device belongs to.
DNS host name	DNS name of the computer.
Remote boot	Specifies whether this device uses remote booting. The property is available if the Hardware Display MachineWithRPL configuration parameter is set.
Remote boot type	Data for the remote boot type. The property is available if the Hardware Display MachineWithRPL configuration parameter is set.

Assigning company resources to devices

One Identity Manager uses different assignment types to assign company resources.

- Indirect assignment

In the case of indirect assignment of company resources, employees, devices, and workdesks are arranged in departments, cost centers, locations, business roles, or application roles. The total of assigned company resources for an employee, device, or workdesk is calculated from the position within the hierarchies, the direction of inheritance (top-down or bottom-up) and the company resources assigned to these roles. In the Indirect assignment methods a difference between primary and secondary assignment is taken into account.

- Direct assignment

Direct assignment of company resources results from the assignment of a company resource to an employee, device, or workdesk, for example. Direct assignment of company resources makes it easier to react to special requirements.

- Assignment by dynamic roles

Assignment through dynamic roles is a special case of indirect assignment. Dynamic roles are used to specify role memberships dynamically. Employees, devices, and workdesks are not permanently assigned to a role, just when they fulfill certain conditions. A check is performed regularly to assess which employees, devices, or workdesks fulfill these conditions. This means the role memberships change dynamically. For example, company resources can be assigned dynamically to all employees in a department in this way; if an employee leaves the department they immediately lose the resources assigned to them.

The following table shows the possible company resources assignments to devices.

NOTE: Company resources are defined in One Identity Manager modules and are not available until the modules are installed.

Table 52: Possible assignments of company resources to devices

Company resources	Direct assignment permitted	Indirect assignment permitted	Comment
Active Directory groups	-	+	All Active Directory computers that reference this device are added to Active Directory groups.
LDAP groups	-	+	All LDAP computers that reference this device are added to LDAP groups.

NOTE: Devices also obtain company resources from their workdesks.

Detailed information about this topic

- [Basic principles for assigning company resources](#) on page 15
- [Permitting assignments of employees, devices, workdesks, and company resources to roles](#) on page 29

Related topics

- [Possible assignments of company resources through roles](#) on page 25
- [Assigning devices to departments, cost centers, and locations](#) on page 168
- [Assigning devices to business roles](#)
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 81
- [Assigning company resources to departments, cost centers, and locations](#) on page 82
- [Assigning company resources to workdesks](#) on page 174
- [Dynamic roles](#) on page 35

Assigning devices to departments, cost centers, and locations


Assign devices to departments, cost centers, and locations so that they obtain company resources through these organizations. To assign company resources to departments, cost centers, and locations, use the appropriate organization tasks.

To assign a device to departments, cost centers, and locations (secondary assignment; default method)

1. In the Manager, select the **Device & Workdesks > Basic configuration data > <filter>** category.
2. Select the device in the result list.
3. Select the **Assign organizations** task.
4. 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 .
5. Save the changes.

To assign a device to departments, cost centers, and locations (primary assignment)

1. In the Manager, select the **Device & Workdesks > Basic configuration data > <filter>** category.
2. Select the device in the result list.
3. Select the **Change main data** task.
4. Adjust the following main data:
 - **Primary department:** Department to which the device is assigned.
 - **Primary cost center:** Cost center to which the device is assigned.
 - **Primary location:** Location to which the device is assigned.
5. Save the changes.

Related topics

- [Assigning company resources to devices](#) on page 167
- [Assigning company resources to departments, cost centers, and locations](#) on page 82
- [Dynamic roles](#) on page 35
- [Assigning employees to business roles](#) on page 139
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 81

Assigning devices to business roles

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


Assign devices to business roles such that the devices obtain company resources through these business roles. To assign company resources to business roles use the corresponding business role tasks. For more information about working with business roles, see the *One Identity Manager Business Roles Administration Guide*.

To assign a device to business roles (secondary assignment; default method)

1. In the Manager, select the **Device & Workdesks > <filter>** category.
2. Select the device in the result list.
3. Select the **Assign business roles** task.
4. 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 .
5. Save the changes.

To assign a device to business roles (primary assignment)

1. In the Manager, select the **Device & Workdesks > <filter>** category.
2. Select the device in the result list.
3. Select the **Change main data** task.
4. In the **Primary business role** menu, select the business role to assign to the device.
5. Save the changes.

Related topics

- [Assigning company resources to devices](#) on page 167

Displaying the device overview

Use this task to obtain an overview of the most important information about a device.

To obtain an overview of a device

1. In the Manager, select the **Device & Workdesks > Basic configuration data > <filter>** category.
2. Select the device in the result list.
3. Select the **Device overview** task.

Entering service agreements and calls for devices

| NOTE: This function is only available if the Helpdesk Module is installed.

Use the Helpdesk Module to enter service agreements and calls for a device. For more information about the help desk, see *One Identity Manager Help Desk Module User Guide*.

To enter help desk data for a device

1. In the Manager, select the **Device & Workdesks > Basic configuration data > <filter>** category.
2. Select the device in the result list.
3. Select the **Assign service agreements** task to assign the valid service agreements to the device.

The service agreements are taken into account when calculating solution and reaction times in the case of a help desk call for this device.


4. Select the **Show calls** task to display calls entered for a device.
5. Select the **New call** task, to enter a new call.
6. Save the changes.

Creating and editing workdesks

Workdesks are used to assign various devices to a workstation or a server. The assignment of company resources can be mainly automated by assigning workdesks to business roles, departments, cost centers, locations, or dynamic roles.

TIP: To create a workdesk automatically when you create a device for a workstation or a server, set the **Hardware | Workdesk | WorkdeskAuto** configuration parameter in the Designer.

To create or edit a workdesk

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. In the result list, select a workdesk and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the workdesk's main data.
4. Save the changes.

Detailed information about this topic

- [General main data of workdesks](#) on page 171
- [Location information for workdesks](#) on page 173
- [Additional information for workdesks](#) on page 173
- [Assigning company resources to workdesks](#) on page 174
- [Configuration parameters for managing devices and workdesks](#) on page 214

General main data of workdesks

Enter the following general main data of a workdesk.

Table 53: General main data of a workdesk

Property	Description
Workdesk	Workdesk name.

Property	Description
	If the Hardware Workdesk WorkdeskAuto configuration parameter is set, a workdesk bearing the same name is automatically created when a workstation or a server is set up.
Workdesk type	Type of the workdesk.
Status	Status of the workdesk.
Display name	The display name is used to display the workdesk in the One Identity Manager tools user interface.
Description	Text field for additional explanation.
Primary cost center	Cost center to which the workdesk is primary assigned. A workdesk can obtain company resources over the primary assignments when One Identity Manager is correspondingly configured.
Primary business roles	Business role to which the employee is assigned. A workdesk can obtain company resources over the primary assignments when One Identity Manager is correspondingly configured. NOTE: This property is available if the Business Roles Module is installed.
Installation date	Date of going into operation.
Workdesk supervisor	Employee responsible for this workdesk.
Checked by	Employee who checked this workdesk.
Date checked	Last time the workdesk was checked.
Check remarks	Text field for additional explanation.
Service type	Information about the service done on this workdesk, for example, internal, or external service provider.
Corresponding service agreements set up	Specifies whether the workdesk is set up according to the service agreements. NOTE: This property is available if the Helpdesk Module is installed.
No inheritance	Specifies whether the workdesk inherits company resources through roles. If this option is set, the employee cannot inherit. Direct assignments remain intact.
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.

Related topics

- [Creating and editing workdesk types](#) on page 160
- [Creating and editing workdesk statuses](#) on page 160
- [Basic principles for assigning company resources](#) on page 15
- [Preventing inheritance to individual employees, devices, or workdesks](#) on page 31

Location information for workdesks

Enter the following information about a workdesk's location.

Table 54: Workdesk location information

Property	Description
Primary department	Department to which the workdesk is primary assigned. A workdesk can obtain company resources over the primary assignments when One Identity Manager is correspondingly configured.
Primary location	Location to which the workdesk is primary assigned. A workdesk can obtain company resources over the primary assignments when One Identity Manager is correspondingly configured.
Fax	Fax number.
Remarks (fax)	Text field for additional explanation.
Building	Building
Room	Room.
Phone	Telephone number.
Floor	Floor.
Remarks (room)	Text field for additional explanation.

Related topics

- [Basic principles for assigning company resources](#) on page 15

Additional information for workdesks

Enter additional device prerequisites are diskettes or CD drives necessary, for example.

Table 55: Miscellaneous workdesk data

Property	Description
Setup date	Date of going into operation.
Withdrawal date	Date on which the workdesk is written off.
Leasing fee	Leasing fee.
Floppy disk drive required	Specifies whether this workdesk requires a floppy disk drive.
CD-ROM drive required	Specifies whether this workdesk requires a CD-ROM drive.
Comment	Text field for additional explanation.

Assigning company resources to workdesks

One Identity Manager uses different assignment types to assign company resources.

- Indirect assignment

In the case of indirect assignment of company resources, employees, devices, and workdesks are arranged in departments, cost centers, locations, business roles, or application roles. The total of assigned company resources for an employee, device, or workdesk is calculated from the position within the hierarchies, the direction of inheritance (top-down or bottom-up) and the company resources assigned to these roles. In the Indirect assignment methods a difference between primary and secondary assignment is taken into account.

- Direct assignment

Direct assignment of company resources results from the assignment of a company resource to an employee, device, or workdesk, for example. Direct assignment of company resources makes it easier to react to special requirements.

- Assignment by dynamic roles

Assignment through dynamic roles is a special case of indirect assignment. Dynamic roles are used to specify role memberships dynamically. Employees, devices, and workdesks are not permanently assigned to a role, just when they fulfill certain conditions. A check is performed regularly to assess which employees, devices, or workdesks fulfill these conditions. This means the role memberships change dynamically. For example, company resources can be assigned dynamically to all employees in a department in this way; if an employee leaves the department they immediately lose the resources assigned to them.

- Assignment by request

Assignment through the IT Shop is a special case of indirect assignment. Add employees to a shop as customers so that company resources can be assigned through IT Shop requests. All company resources assigned as product to this shop

can be requested by the customers. Requested company resources are assigned to the employees after approval is granted. Role memberships can be requested through the IT Shop as well as company resources.

For more information about requests for workdesks, see the *One Identity Manager IT Shop Administration Guide* and the *One Identity Manager Web Portal User Guide*.

The following table shows the possible company resources assignments to workdesks.

NOTE: Company resources are defined in One Identity Manager modules and are not available until the modules are installed.

Table 56: Possible assignments of company resources to workdesks

Company Resource	Direct assignment permitted	Indirect assignment permitted	Remarks
System roles	+	+	
Software	+	+	
Active Directory groups	-	+	All Active Directory computers that reference the workdesk device are added to Active Directory groups.
LDAP groups	-	+	All LDAP computers that reference the workdesk device are added to LDAP groups.

Detailed information about this topic

- [Basic principles for assigning company resources](#) on page 15
- [Permitting assignments of employees, devices, workdesks, and company resources to roles](#) on page 29

Related topics

- [Possible assignments of company resources through roles](#) on page 25
- [Assigning workdesks to departments, cost centers, and locations](#) on page 176
- [Assigning workdesks to business roles](#)
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 81
- [Assigning company resources to departments, cost centers, and locations](#) on page 82
- [Dynamic roles](#) on page 35

Assigning workdesks to departments, cost centers, and locations


Assign workdesks to departments, cost centers, and locations so that they obtain company resources through these organizations. To assign company resources to departments, cost centers, or locations, use the appropriate organization tasks.

To assign a workdesk to departments, cost centers, and locations (secondary assignment; default method)

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select the **Assign organizations** task.
4. 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 .
5. Save the changes.

To assign a workdesk to departments, cost centers, and locations (primary assignment)

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select the **Change main data** task.
4. Adjust the following main data:
 - **Primary department:** Department to which the workdesk is assigned.
 - **Primary cost center:** Cost center to which the workdesk is assigned.
 - **Primary location:** Location to which the workdesk is assigned.
5. Save the changes.

Related topics

- [Assigning company resources to workdesks](#) on page 174
- [Assigning company resources to departments, cost centers, and locations](#) on page 82

- [Dynamic roles](#) on page 35
- [Assigning devices to business roles](#) on page 169
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 81

Assigning workdesks to business roles

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


Assign the workdesk to business roles so that the workdesk obtains its company resources through these business roles. To assign company resources to business roles use the corresponding business role tasks. For more information about working with business roles, see the *One Identity Manager Business Roles Administration Guide*.

To assign a workdesk to business roles (secondary assignment; default method)

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select the **Assign business roles** task.
4. 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 .
5. Save the changes.

To assign a workdesk to business roles (primary assignment)

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select the **Change main data** task.
4. In the **Primary business role** menu, select the business role to assign to the workdesk.
5. Save the changes.

Related topics

- [Assigning company resources to workdesks](#) on page 174

Assigning software directly to workdesks

NOTE: This function is only available if the Software Management Module is installed.

Software can be assigned directly or indirectly to a workdesk. Indirect assignment is carried out by assigning workdesks and software to company structures, such as departments, locations, or business roles.


To react quickly to special requests, you can assign software directly to a workdesk.

To assign software to a workdesk

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select the **Assign software** task.
4. In the **Add assignments** pane, assign software.

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

To remove an assignment

- Select the software and double-click .
5. Save the changes.

Related topics

- [Assigning workdesks to departments, cost centers, and locations](#) on page 176
- [Assigning workdesks to business roles](#) on page 177

Assigning system roles directly to workdesks

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

System roles can be assigned directly or indirectly to a contact. Indirect assignment is carried out by assigning workdesks and system roles to company structures, such as departments, cost centers, locations, or business roles. For more information about working with system roles, see the *One Identity Manager System Roles Administration Guide*.

To react quickly to special requests, you can assign system roles directly to a workdesk.

To assign system roles to a workdesk

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select the **Assign system roles** task to assign system roles directly to the workdesk.
4. In the **Add assignments** pane, assign system roles.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click ✓.
5. Save the changes.

Related topics

- [Assigning workdesks to departments, cost centers, and locations](#) on page 176
- [Assigning workdesks to business roles](#) on page 177

Displaying the workdesk overview

Use this task to obtain an overview of the most important information about a workdesk.

To obtain an overview of a workdesk

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select the **Workdesk overview** task.

Assigning devices to workdesks


Use this task to assign a workdesk to several devices, for example, workstations, printers, monitors, or other peripheral devices. You can also assign the workdesk through the device's main data.

To assign devices to a workdesk

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select the **Assign devices** task.
4. In the **Add assignments** pane, assign the devices.

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

To remove an assignment

- Select the device and double-click .
5. Save the changes.

Related topics

- [General main data for devices](#) on page 163

Assigning workdesks to employees


Use this task to assign a workdesk to several employees. You can also assign the workdesk through the employee's main data.

To assign a workdesk to employees

1. In the Manager, select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select the **Assign employees** task.
4. In the **Add assignments** pane, add employees.

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

To remove an assignment

- Select the employee and double-click .
5. Save the changes.

Related topics

- [General employee main data](#) on page 119

Entering calls for workdesks

| NOTE: This function is only available if the Helpdesk Module is installed.

Use the Helpdesk Module to enter service agreements and calls for a workdesk. For more information about the help desk, see *One Identity Manager Help Desk Module User Guide*.

To enter help desk data for a workdesk

1. Select the **Devices & Workdesks > Workdesks > Names** category.
2. Select the workdesk in the result list.
3. Select **Show calls**, to show the calls entered for a workdesk.
4. Select the **New call** task, to enter a new call.
5. Save the changes.

Asset data for devices

One Identity Manager offers the possibility for the administration of data for assets and accounting within the framework of inventory management. Further information about business partners, ownership (leasing, purchasing, renting) and the associated contract information about cost and time periods belongs here. For the assets inventory management, data can be taken from another system and adopted by the One Identity Manager. For example a file extracted from the SAP R/3 assets accounting can act as data source.

To use this function

- In the Designer, set the **Hardware | AssetAccounting** configuration parameter and compile the database.

| NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not 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*.


Detailed information about this topic

- [Creating and editing asset classes for devices](#) on page 182
- [Creating and editing asset types for devices](#) on page 182
- [Basic data for device admin](#) on page 155
- [Entering investments and investment plans for devices](#) on page 183
- [Editing device asset data](#) on page 183
- [Configuration parameters for managing devices and workdesks](#) on page 214

Creating and editing asset classes for devices

Enter asset classes for asset data about a device.

To edit or create an asset class

1. In the Manager, select the **Devices & Workdesks > Basic configuration data > Asset classes** category.
2. In the result list, select an asset class and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the asset class's main data.
4. Save the changes.

Enter the following data for an asset class.


Table 57: Asset class main data

Property	Description
Storage class	Description of the asset class.
Display name	Name for displaying in the One Identity Manager tools.
Description	Text field for additional explanation.

Creating and editing asset types for devices

Enter asset types for asset data about a device.

To create or edit an asset type

1. In the Manager, select the **Devices & Workdesks > Basic configuration data > Asset types** category.
2. In the result list, select an asset type and run the **Change main data** task.
- OR -
Click  in the result list.
3. Enter the name of the asset type and a description for additional explanation.
4. Save the changes.

Entering investments and investment plans for devices

Enter the data for investments and investment plans and assign them to devices.

To create or edit an investment


1. In the Manager, select the **Devices & Workdesks > Investments category**.
2. In the result list, select an investment and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the following main data.

Table 58: Investments main data

Property	Description
Investment	Name of the investment plan.
Date	Date of investment.
Investment manager	Employee responsible for the investment.
Description	Text field for additional explanation.
Remarks	Text field for additional explanation.

4. Save the changes.

Related topics

- [General main data for devices](#) on page 163

Editing device asset data

To edit a device's asset information

1. In the Manager, select the **Device & Workdesks > Basic configuration data > <filter>** category.
2. Select the device in the result list.
3. Select the **Edit asset data** task.
4. Edit the asset data's main data.
5. Save the changes.

Detailed information about this topic

- [Main data for devices' asset data](#) on page 184
- [Commercial data for devices](#) on page 185

Main data for devices' asset data

Enter the following main data of the asset data of a device.

NOTE: Prices are given to 2 decimal places by default. The number of decimal places to enter can be modified in the Designer. For more information, see the *One Identity Manager Configuration Guide*.

Table 59: Device asset data

Property	Description
Asset number	Number of the asset in the bookkeeping.
Asset	Asset.
Storage class	Asset class.
Storage type	Asset type.
Device status	The device's status.
Enabling	Date for enabling the asset or beginning the lease, respectively.
Deactivation	Date for disabling the asset or end of lease, respectively.
Replacement value	Value for replacing with a new device.
Depreciated value	Depreciation value for the device.
Company owned	Specifies whether the device is owned by the company.
Leased	Specifies whether the device is leased.
Invoice number	Invoice number of the purchase.
PSP character string	Asset PSP as character string.
Last inventory run	Date of last inventory.
Primary cost center	Cost center. Company resources can be inherited by a device through these primary assignments if One Identity Manager is appropriately configured.

Property	Description
Serial number	Serial number of the device.
Delivery remarks	Text field for additional explanation.
Inventory remarks	Text field for additional explanation.
Primary business role	Business role. A workdesk can obtain company resources over the primary assignments when One Identity Manager is correspondingly configured. NOTE: This property is available if the Business Roles Module is installed.
Primary location	Location. Company resources can be inherited by a device through these primary assignments if One Identity Manager is appropriately configured.
Primary department	Department. Company resources can be inherited by a device through these primary assignments if One Identity Manager is appropriately configured.

Related topics

- [Creating and editing asset classes for devices](#) on page 182
- [Creating and editing asset types for devices](#) on page 182
- [Basic principles for assigning company resources](#) on page 15

Commercial data for devices

Enter the following asset data for a device.

NOTE: Prices are given to 2 decimal places by default. The number of decimal places to enter can be modified in the Designer. For more information, see the *One Identity Manager Configuration Guide*.

Table 60: Commercial data of a device

Property	Description
Acquisition date	Date of purchase.
Delivery date	Date of delivery.
Delivery voucher number	Delivery voucher number.

Property	Description
Voucher	Voucher. For more information about vouchers, see the <i>One Identity Manager Chargeback Administration Guide</i> .
Warranty	Warranty expiry date.
Warranty number	Warranty number.
Setup date	Date of going into operation.
Owner	Leasing company.
supplier	Name of supplier.
Manufacturer	Name of manufacturer.
Purchase price	Purchase price.
Internal price	Internal price.
Sales price	Sales price.
Currency	Currency unit
Inventory note	Text field for additional explanation.
Withdrawal date	Date for writing off the device.
Investment	Investment or investment plan.
Leasing fee	Leasing fee.
Internal transfer price	Internal transfer price.
Depreciation month	Depreciation in months

Related topics

- [Creating and editing business partners on page 158](#)
- [Entering investments and investment plans for devices on page 183](#)

Managing resources

One Identity Manager not only offers the possibility to map IT resources but also non-IT resources such as mobile telephones, desks, company cars, and keys: in other words, everything that is necessary to create an efficient working environment for an employee. You can assign resources directly to an employee or through classification into hierarchical roles in the One Identity Manager. Similarly, you can resources request for an employee through the IT Shop.

Resources are divided up from a functional point of view.

Table 61: Resource types

Type	Description	Table
Resources	Resources that an employee (workdesk, device) may own just once. The resources can be requested in the IT Shop just once. The resources are assigned to the employees 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.	QERRResource
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 employees. Example: resource for requesting remote desktop sessions for assets in a PAM system; consumables, such as pens, printing paper.	QERRReuse
Multi requestable/unsubscribable resources	Resources that an employee can request more than once in the IT Shop but must return them explicitly once they are no	QERRReuseUS

Type	Description	Table
	longer needed. The resources are assigned to the employees after approval has been granted. They remain assigned until the request is canceled. Example: printer, monitor.	
Assignment resources	Assignment resources are special resources for requesting any number of assignments to hierarchical roles or to delegate responsibilities in the IT Shop. For more information about assignment resources, see the <i>One Identity Manager IT Shop Administration Guide</i> .	QERAssign

Detailed information about this topic

- [Creating and editing resources](#) on page 190
- [Assigning resources to employees](#) on page 192
- [Creating and editing multi-request resources](#) on page 196
- [Assigning multi-request resources to employees](#) on page 198
- [Reports about resources](#) on page 201

One Identity Manager users for managing resources

The following users are used for user administration.

Table 62: 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: <ul style="list-style-type: none"> • Edit the resources and assign them to IT Shop structures.
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:

Users	Tasks
	<ul style="list-style-type: none"> • 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. • Create and configure password policies as required.

Basic data for resources

The following basic data is required for managing resources.

- Resource types
You can use resource types to group resources.
- Extended properties
Extended properties are meta objects, such as operating codes, cost codes, or cost accounting areas that cannot be mapped directly in One Identity Manager.


Detailed information about this topic

- [Resource types](#) on page 189
- [Creating and editing extended properties](#) on page 204

Resource types

You can use resource types to group resources.


To create or edit resource types

1. In the Manager, select the **Entitlements > Basic configuration data > Resource types** category.
2. In the result list, select an resource type and run the **Change main data** task.
 - OR –
 - Click  in the result list.

3. Enter a name and description for the resource type.
4. Save the changes.

Creating and editing resources

To create or edit resources

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a resource in the result list and run the **Change main data** task.
 - OR -
 - Click  in the result list.
3. Edit the resource's main data.
4. Save the changes.

Detailed information about this topic

- [Main data for resources](#) on page 190
- [Assigning resources to employees](#) on page 192

Main data for resources

Enter the following main data of a resource.

Table 63: Resource main data

Property	Description
Resource	Resource identifier.
Resource type	Resource type for grouping resources.
Service item	Service item through which you can request the resource in the IT Shop. Assign an existing service item or add a new one.
Required resource	Define the dependencies between resources. When this resource is requested or assigned, the required resource is assigned automatically.
Risk index	Value for evaluating the risk of assigning the resource to employees. Set a value in the range 0 to 1 . This input field is only visible if the QER CalculateRiskIndex configuration parameter is set.

Property	Description
	For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
IT Shop	<p>Specifies whether the resource can be requested through the IT Shop. The resource can be requested by an employee through the Web Portal and distributed using a defined approval process. The resource can still be assigned directly to employees and roles outside of the IT Shop.</p> <p>For more information, see the <i>One Identity Manager IT Shop Administration Guide</i>.</p>
Only for use in IT Shop	<p>Specifies whether the resource can be requested through the IT Shop. The resource can be requested by an employee through the Web Portal and distributed using a defined approval process. The resource cannot be directly assigned to roles outside the IT Shop.</p> <p>For more information, see the <i>One Identity Manager IT Shop Administration Guide</i>.</p>
No inheritance on security risk	Resources marked with this option are not inherited by employee who are rated as a security risk.
Description	Text field for additional explanation.
Automatic assignment to employees	<p>Specifies whether the resource is automatically assigned to all internal employees. By saving the resource, it is assigned to every employee that is not marked as external. Once a new internal employee is created, they automatically obtain this resource.</p> <p>To automatically remove the resource assignment from all employees, disable this option. The resource cannot be reassigned to employees from this point on. Existing resource assignments remain intact.</p>
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.

Related topics

- [Resource types](#) on page 189
- [General employee main data](#) on page 119
- [Calculation of assignments](#) on page 22

Assigning resources to employees

Resources can be assigned to employees directly, indirectly, or through IT Shop requests. In the case of indirect assignment employees and resources are arranged in hierarchical roles. The number of resources assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance. Add employees to a shop as customers so that resources can be assigned through IT Shop requests. All resources, which are assigned to this shop can be requested by the customers. Requested resources are assigned to the employees after approval is granted.

The prerequisite for indirect assignment of resources to employees is:

- Assignment of employees and resources is permitted for role classes (departments, cost centers, locations, or business roles).

Detailed information about this topic

- [Permitting assignments of employees, devices, workdesks, and company resources to roles](#) on page 29
- [Basic principles for assigning company resources](#) on page 15

Assigning resources to departments, cost centers, and locations


Assign a resource to departments, cost centers or locations such that employees inherit the resource through these organizations.

To assign a resource to departments, cost centers and locations

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a resource in the result list.
3. Select the **Assign organizations** task.
4. 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 .
5. Save the changes.

Related topics

- [Departments, cost centers, and locations](#) on page 52
- [Basics for mapping company structures in One Identity Manager](#) on page 10

Assigning resources to business roles

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


Assign a resource to business roles such that the resource is inherited by employees through these business roles. For more information about working with business roles, see the *One Identity Manager Business Roles Administration Guide*.

To assign a resource to business roles

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a resource in the result list.
3. Select the **Assign business roles** task.
4. 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 .
5. Save the changes.

Assigning resources directly to employees

Resources can be assigned directly or indirectly to employees. Indirect assignment is carried out by allocating employees and resources in company structures, like departments, cost centers, locations, or business roles.


To react quickly to special requests, you can assign resources directly to employees.

To assign a resource directly to employees

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a resource in the result list.
3. Select the **Assign to employees** task.
4. In the **Add assignments** pane, add employees.

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

To remove an assignment

- Select the employee and double-click .
5. Save the changes.

Related topics

- [Employee administration](#) on page 92
- [Basic principles for assigning company resources](#) on page 15

Adding resources to the IT Shop

Once a resource has been assigned to an IT Shop shelf, it can be requested by the shop customers. There are other prerequisites required to make a resource requestable.

- The resource must be labeled with the **IT Shop** option.
- The resource must be assigned to a service item.
- The resource must be also labeled with the **Only use in IT Shop** option if it is only to be assigned to employees by means of IT Shop requests. Then, the resource may not be assigned directly to hierarchical roles.

For more information about requesting company resources through the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

To add a resource to the IT Shop

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a resource in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the resource to the IT Shop shelves.
5. Save the changes.

To remove a resource from individual IT Shop shelves

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a resource in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the resource from the IT Shop shelves.
5. Save the changes.

To remove resource from all IT Shop shelves

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a 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 resource is removed from all shelves by the One Identity Manager Service. All requests and assignment requests that include this resource are canceled in the process.

Related topics

- [Main data for resources](#) on page 190

Adding resources in system roles

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

A resource can be added to different system roles. A system role that only contains resources can be labeled with the **Resource package** system role type. Resources can also be added to system roles that are not resource packages. When you assign a system role to an employee the resource is assigned to the employee.

For more information about working with system roles, see the *One Identity Manager System Roles Administration Guide*.


NOTE: Resources with the **Only use in IT Shop** option set can only be assigned to system roles that also have this option set.

To assign a resource to system roles

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a resource in the result list.
3. Select the **Assign system roles** task.
4. In the **Add assignments** pane, assign system roles.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click .
5. Save the changes.

Displaying the resources overview

Use this task to obtain an overview of the most important information about a resource. The affiliation of the resource to hierarchical roles and IT Shop structures counts in this

here.

To obtain an overview of a resource

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a resource in the result list.
3. Select the **Resource overview** task.

Assigning extended properties to resources


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 specify extended properties for an resource

1. In the Manager, select the **Entitlements > Resources** category.
2. Select a resource in the result list.
3. Select **Assign extended properties**.
4. 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 .
5. Save the changes.

Detailed information about this topic


- [Creating and editing extended properties](#) on page 204

Creating and editing multi-request resources


You can only edit multi-request resources if the **QER | ITShop** configuration parameter is set.

- In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.

To create or edit multi-request resources

1. In the Manager, select the **Entitlements > Multi-request resources for IT Shop** category.
2. Select a resource in the result list and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the multi-request resource's main data.
4. Save the changes.

To create or edit multi requestable/unsubscribable resources

1. In the Manager, select the **Entitlements > Multi requestable/unsubscribable resources for IT Shop** category.
2. Select a resource in the result list and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the multi requestable/unsubscribable resource's main data.
4. Save the changes.

Detailed information about this topic

- [Main data for multi-request resources](#) on page 197
- [Assigning multi-request resources to employees](#) on page 198
- [Adding multi-request resources to the IT Shop](#) on page 199

Main data for multi-request resources

Enter the following main data of a multi-request resource.

Table 64: Main data for a multi-request resource

Property	Description
Multi-request resource	Resource identifier.
Multi requestable/unsubscribable resource	
Resource type	Resource type for grouping resources.
Service item	Service item through which you can request the resource in the IT Shop. Assign an existing service item or add a new one.

Property	Description
Risk index	<p>Value for evaluating the risk of assigning the resource to employees. Set a value in the range 0 to 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set.</p> <p>For more information, see the <i>One Identity Manager Risk Assessment Administration Guide</i>.</p>
IT Shop	<p>Specifies whether the resource can be requested through the IT Shop. The resource can be requested by an employee through the Web Portal and distributed using a defined approval process. The resource can still be assigned directly to employees and roles outside of the IT Shop.</p> <p>This option cannot be disabled. For more information, see the <i>One Identity Manager IT Shop Administration Guide</i>.</p>
Only for use in IT Shop	<p>Specifies whether the resource can be requested through the IT Shop. The resource can be requested by an employee through the Web Portal and distributed using a defined approval process. The resource cannot be directly assigned to roles outside the IT Shop.</p> <p>This option cannot be disabled. For more information, see the <i>One Identity Manager IT Shop Administration Guide</i>.</p>
Description	Text field for additional explanation.
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.

Related topics

- [Resource types](#) on page 189

Assigning multi-request resources to employees

Assign multi requestable resources through IT Shop requests to employees. To do this, add employees to a shop as customers. All resources, which are assigned to this shop can be requested by the customers. For more information, see the *One Identity Manager IT Shop Administration Guide*.


Detailed information about this topic

- [Adding multi-request resources to the IT Shop on page 199](#)
- [Assigning company resources through IT Shop requests on page 19](#)

Adding multi-request resources to the IT Shop

A multi-request resource can be requested by shop customers when it is assigned to an IT Shop shelf. For more information, see the *One Identity Manager IT Shop Administration Guide*.


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.


In the **Add assignments** pane, assign a shelf.

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.

In the **Add assignments** pane, assign a shelf.

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 remove multi-request resources from all IT Shop shelves

1. In the Manager, select the **Entitlements > Multi-request resources for IT Shop** category.

- OR -

In the Manager, select the **Entitlements > Multi requestable/unsubscribable resources for IT Shop** category.

2. Select a 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 resource is removed from all shelves by the One Identity Manager Service. This cancels all requests for this resource.

Displaying the multi-request resource overview

Use this task to obtain an overview of the most important information about a multi-request resource. For this, take into account the affiliation of the resource to IT Shop structures.

To obtain an overview of a multi-request resource

1. In the Manager, select the **Entitlements > Multi-request resources for IT Shop** category.
2. Select a resource in the result list.
3. Select the **Multi-Request resource overview** task.

To obtain an overview of a requestable/unsubscribable resource

1. In the Manager, select the **Entitlements > Multi requestable/unsubscribable resources for IT Shop** category.
2. Select a resource in the result list.
3. Select the **Multi requestable/Unsubscribable resource overview** task.

Reports about resources

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 resources.

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

Table 65: Reports about resources

Report	Description
Overview of all assignments	This report finds all roles containing employees with the selected resource.

Related topics

- [Analyzing role memberships and employee assignments](#) on page 145

Setting up extended properties

Extended properties are meta objects, such as operating codes, cost codes, or cost accounting areas that cannot be mapped directly in One Identity Manager. You can assign extended properties to company resources, hierarchical roles, and employees. They can, for example, be used in the rule conditions of compliance rules.

To assign extended properties

1. First, set up a property group, under which the extended properties will be grouped.
2. Set up the extended properties in the property group.
3. Assign the extended properties to the objects.

There can be any number of objects of different object types assigned to an extended property at this point.

Detailed information about this topic

- [Creating property groups for extended properties](#) on page 203
- [Creating and editing extended properties](#) on page 204

One Identity Manager users for managing extended properties

The following users are used for managing extended properties.

Table 66: 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:

Users	Tasks
	<ul style="list-style-type: none"> • Create extended properties for company resources of any type.
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> • 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. • Create and configure password policies as required.

Creating property groups for extended properties

Property groups are used to group extended properties. Each extended property must be assigned to at least one property group. Furthermore, you can assign the extended properties to any other property groups.

To create a property group


1. In the Manager, select the **Entitlements > Basic configuration data > Extended properties** category.
2. Click  in the result list.
3. Enter a name and description for the property group.
4. Save the changes.

Related topics

- [Assigning extended properties to property groups](#) on page 205
- [Main data for extended properties](#) on page 204
- [Assigning additional property groups to extended properties](#) on page 206

Creating and editing extended properties

To edit an extended property

1. In the Manager, select the **Entitlements > Basic configuration data > Extended properties > <property group>** category.
2. Select the extended property in the result list. Select the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the extended property's main data.
4. Save the changes.

Detailed information about this topic

- [Main data for extended properties](#) on page 204
- [Specifying scope limits for extended properties](#) on page 206

Main data for extended properties

Enter the following data for an extended property.

Table 67: Extended property main data

Property	Description
Extended property name	Name of the extended property.
Property group	The property group for structuring extended properties. You can assign a primary property group to a property on the main data form. Extended properties are grouped by this property group in navigation. If you have to assign an extended property to several property groups, you can assign additional property groups.
Lower scope limit	Lower scope limit for further subdivision.
Upper scope limit	Upper scope limit for further subdivision.

Property	Description
Description	Text field for additional explanation.
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.

Related topics

- [Specifying scope limits for extended properties on page 206](#)
- [Assigning additional property groups to extended properties](#)
- [Assigning extended properties to property groups](#)

Assigning extended properties to property groups

Each extended property must be assigned to at least one property group. Furthermore, you can assign the extended properties to any other property groups.


If you want to assign more properties to a property group, use the **Assign extended properties** task.

To assign extended properties to a property group

1. In the Manager, select the **Entitlements > Basic configuration data > Extended properties** category.
2. Select a property group in the result list.
3. Select the **Assign extended properties** task.
4. 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 .
5. Save the changes.

Related topics

- [Main data for extended properties on page 204](#)
- [Assigning additional property groups to extended properties on page 206](#)

Assigning additional property groups to extended properties


Each extended property must be assigned to at least one property group. Furthermore, you can assign the extended properties to any other property groups. If an extended property needs to be assigned to several property groups, then you can use the **Assign property groups** task to assign additional property groups.

To assign an extended property to a property group

1. In the Manager, select the **Entitlements > Basic configuration data > Extended properties > <property group>** category.
2. Select the extended property in the result list.
3. Select the **Assign property groups** task.
4. In the **Add assignments** pane, assign property groups.

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

To remove an assignment

- Select the property group and double-click .
5. Save the changes.

Related topics

- [Main data for extended properties](#) on page 204
- [Assigning extended properties to property groups](#) on page 205

Specifying scope limits for extended properties

You can subdivide extended properties by specifying scoped limits. You are not obliged to enter scoped limit. If you do enter a lower boundary you are not required to enter an upper one. However, if you specify an upper boundary, you have to enter a lower one.

Take note of the following when defining scoped limits:

- Basically, any string is permitted as a lower or upper scoped limit.
- You can use ***** as a wildcard for any number of characters (even null).
- Wild cards can only be added to the end of a string, for example, **AB***. Strings such as ***AB** or **A*B** are not allowed, for example.

- If you enter a lower boundary without a wildcard, you cannot use a wildcard in the upper boundary.

The following restrictions apply for the length of the string:

- If you enter a lower and upper boundary without a wildcard, the strings have to be the same length, for example, lower boundary 123/upper boundary 456. A lower boundary of 123 and an upper of 45, for example, is not permitted or a lower boundary 123/upper boundary 4567 is also not allowed.
- If you use a wildcard in the lower boundary but none in the upper boundary, then the length of the upper boundary string needs to be the same as or bigger than the string in the lower boundary.
- If you use a wildcard in the lower and upper boundary, they have to be the same length, for example, lower boundary 123*/upper boundary 456*. A lower boundary of 123* and an upper of 45*, for example, is not permitted or a lower boundary 123*/upper boundary 4567* is also not allowed.

Displaying the extended properties overview

Use this task to obtain an overview of the most important information about an extended property. For this you need to take into account the affiliation of the extended property to the different One Identity Manager objects.

To obtain an overview of an extended property

1. In the Manager, select the **Entitlements > Basic configuration data > Extended properties > <property group>** category.
2. Select the extended property in the result list.
3. Select the **Extended property overview** task.

To obtain an overview of a property group

1. In the Manager, select the **Entitlements > Basic configuration data > Extended properties** category.
2. Select a property group in the result list.
3. Select the **Property group overview** task.

Assigning objects to extended properties


You can assign extended properties to company resources, hierarchical roles, and employees.

To assign objects to an extended property

1. In the Manager, select the **Entitlements > Basic configuration data > Extended properties > <property group>** category.
2. Select the extended property in the result list.
3. Select the **Assign objects** task.
4. In the **Table** menu, select the required object type.
The object belonging to the object types are displayed on the form.
5. In the **Add assignments** pane, assign objects.

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

To remove an assignment

- Select the object and double-click .
6. Save the changes.

Configuration parameters for managing departments, cost centers, and locations

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 68: Configuration parameter

Configuration parameters	Description
QER Structures	Controls whether hierarchical roles are supported.
QER Structures DynamicGroupCheck	Controls generation of calculation tasks for dynamic roles. If the configuration parameter is not set, the subparameters do not apply.
QER Structures DynamicGroupCheck CalculateImmediatelyPerson	If the parameter is set, a calculation task for modifications to employees or employee level objects is queued immediately in the DBQueue Processor. If the parameter is not set, the calculation tasks are queued the next time the schedule is planned to run.
QER Structures DynamicGroupCheck CalculateImmediatelyHardware	If the parameter is set, a calculation task for modifications to employees or employee level objects is queued immediately in the DBQueue Processor. If the parameter is not set, the calculation tasks are queued the next time the schedule is planned to run.
QER Structures DynamicGroupCheck CalculateImmediatelyWorkdesk	If the parameter is set, a calculation task for modifications to workdesks or workdesk level objects is queued immediately in the DBQueue Processor. If the parameter is not set, the calculation tasks are queued the next time the schedule is planned to run.
QER Structures ExcludeStructures	Preprocessor relevant configuration parameter for defining the effectiveness of role memberships. If this parameter is set, mutually excluding roles can be

Configuration parameters	Description
	<p>defined. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not 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 <i>One Identity Manager Configuration Guide</i>.</p>
QER Structures Inherit Employee	Determines whether employees inherit through primary assignment.
QER Structures Inherit Employee GroupExclusion	Specifies whether employees inherit assignments from their primary department (Person.UID_Department).
QER Structures Inherit Employee FromLocality	Specifies whether employees inherit assignments from their primary location (Person.UID_Locality).
QER Structures Inherit Employee FromProfitCenter	Specifies whether employees inherit assignments from their primary cost center (Person.UID_ProfitCenter).
QER Structures Inherit Hardware	Determines whether devices inherit through primary assignment.
QER Structures Inherit Hardware FromDepartment	Specifies whether devices inherit assignments from their primary department (Hardware.UID_Department).
QER Structures Inherit Hardware FromLocality	Specifies whether devices inherit assignments from their primary location (Hardware.UID_Locality).
QER Structures Inherit Hardware FromProfitCenter	Specifies whether devices inherit assignments from their primary cost center (Hardware.UID_ProfitCenter).
QER Structures Inherit Workdesk	Determines whether workdesks inherit through primary assignment.
QER Structures Inherit Workdesk FromDepartment	Specifies whether workdesks inherit assignments from their primary department (Workdesks.UID_Department).
QER Structures Inherit Workdesk FromLocality	Specifies whether workdesks inherit assignments from their primary location (Workdesk.UID_Locality).
QER Structures Inherit Workdesk FromProfitCenter	Specifies whether workdesks inherit assignments from their primary cost center (Workdesk.UID_ProfitCenter).

Configuration parameters for managing employees

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 69: Configuration parameters

Configuration parameter	Description
QER Person	If this configuration parameter is set, employee administration is supported.
QER Person AllowLoginWithSecurityIncident	<p>Specifies whether employees who are classified as security risks are allowed to log in to the One Identity Manager.</p> <p>If the configuration parameter is set, login is possible.</p> <p>If the configuration parameter is not set, employees who are classified as security risk are not allowed to log in (default).</p>
QER Person CentralAccountGlobalUnique	<p>Specifies how the central user account is mapped.</p> <p>If this configuration parameter is set, the central user account for an employee is formed uniquely in relation to the central user accounts of all employees and the user account names of all permitted target systems.</p> <p>If the configuration parameter is not set, it is only formed uniquely related to the central user accounts of all employees.</p>
QER Person DefaultMailDomain	Default mail domain. The value is used to establish an employee's email address.
Person MasterIdentity UseMasterForAuthentication	Specifies whether the main identity should be used to log in to One Identity Manager tools using an employee-linked authentication module.

Configuration parameter	Description
	If this parameter is set, the main identity is used for employee-linked authentication. If the parameter is not set, the subidentity for employee-linked authentication is used.
QER Person PasswordResetAuthenticator InvalidateUsedQuery	Specifies whether the password questions used for a successful password reset become invalid afterward.
QER Person PasswordResetAuthenticator QueryAnswerDefinitions	Specifies the number of password questions that an employee has to define in order to change their password.
QER Person PasswordResetAuthenticator QueryAnswerRequests	Specifies the number of password questions that an employee has to answer in order to change their password.
QER Person PasswordResetAuthenticator PasscodeSplit	Specifies whether a passcode generated by the help desk is split into two components, one for the help desk and one for the employee's manager.
QER Person TemporaryDeactivation	<p>Controls the behavior between employees and user accounts if employees are temporarily deactivated.</p> <p>If the configuration parameter is set, the employee's user accounts are locked if the employee is permanently or temporarily disabled.</p> <p>If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.</p>
QER Person UseCentralPassword	Specifies whether the employee's central password is used in the user accounts. The employee's central password is automatically mapped to the employee's user account in all permitted target systems. This excludes privileged user accounts, which are not updated.
QER Person UseCentralPassword CheckAllPolicies	Specifies whether an employee's central password is checked against all the target system's password policies of the employee's user accounts. Checking is only carried out in the Password Reset Portal.
QER Person UseCentralPassword SyncToSystemPassword	Specifies whether the employee's central password is copied to the employee's system user password.
QER Person UseCentralPassword SyncToSystemPassword	Specifies whether the employee's system user account is unlocked when the central password is synchronized.

Configuration parameter	Description
UnlockByCentralPassword	
SysConfig	Allows configuration of general system behavior settings.
SysConfig Display	Allows the configuration of the front-end design.
SysConfig Display SourceDetective	<p>Preprocessor relevant configuration parameter for controlling how the source of an employee's entitlements are displayed. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not 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 <i>One Identity Manager Configuration Guide</i>.</p>

Configuration parameters for managing devices and workdesks

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 70: Configuration parameter

Configuration parameters	Description
Hardware	<p>Preprocessor relevant configuration parameter to control the database model components for device administration. If the parameter is set, the device administration components are available. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not 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 <i>One Identity Manager Configuration Guide</i>.</p>
Hardware AssetAccounting	<p>Preprocessor parameter to control the model components for asset accounting. If the parameter is set, asset accounting components are available. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not 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 <i>One Identity Manager Configuration Guide</i>.</p>
Hardware Display	<p>Specifies whether the displaying of device properties can be configured.</p>
Hardware Display	<p>Specifies whether forms customized to the main data are</p>

Configuration parameters	Description
CustomHardwareType	displayed when setting up a new device with the appropriate device model.
Hardware Display CustomHardwareType MobilePhone	Add a device type that represents a mobile phone.
Hardware Display CustomHardwareType Monitor	Add a device type that represents a monitor
Hardware Display CustomHardwareType PC	Add a device type that represents a PC.
Hardware Display CustomHardwareType Printer	Add a device type that represents a printer.
Hardware Display CustomHardwareType Server	Add a device type that represents a server.
Hardware Display CustomHardwareType Tablet	Add a device type that represents a tablet.
Hardware Display DisplayResolutions	Pipe delimited list of all monitor resolutions that are supplied on the device's main data forms.
Hardware Display MachineWithRPL	Specifies whether the data for remote booting of workstations and servers can be edited.
Hardware Workdesk	If this configuration parameter is set, workdesk administration is supported.
Hardware Workdesk WorkdeskAuto	Specifies whether when setting up a workstation or server, an associated workdesk is automatically created.
Hardware Workdesk WorkdeskAutoPerson	If this configuration parameter is set, creating a workdesk automatically creates an associated employee object. This employee object can be used to make requests for this workstation.

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

Contacting us

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

Technical support resources

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

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

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

A

- admin identity
 - personal 103
- application role
 - additional manager 53
 - administrators 53, 93
 - approver 53, 62
 - approver (IT) 53, 62
 - assign employees 140
 - attestors 53, 61
 - base roles
 - employee manager 93
 - employee manager 93
 - Identity Management
 - employees
 - administrators 93
- assignment
 - about IT Shop request 19
 - company resources 25
 - direct 16
 - dynamic role 19
 - indirect 16
 - primary 17
 - configurations 17
 - secondary 16
 - configurations 29
 - permit 29

B

- business partner 95, 158

C

- calculation schedule
 - default schedule 40
 - run immediately 43
 - set up 40
- certification 90
- certification status 90
- company resources
 - assign 15, 82, 133, 167, 174
- configuration parameter 211, 214
- cost center
 - administrators 53
 - allow assignment 29
 - approver 62, 68
 - approver (IT) 62, 68
 - assign company resources 25, 82
 - assign devices 81, 168
 - assign employees 81, 138
 - assign extended properties 89
 - assign workdesk 176
 - assign workdesks 81
 - attestors 53, 61, 68
 - basics 11
 - certification status 90
 - conflicting roles 33, 87
 - country 70
 - dynamic 85
 - edit 67
 - functional area 70

- IT operating data 76
- manager 68
- no inheritance 30-31, 68
- profit 70
- risk index 70
- rule violation 70
- short name 68
- state 70
- transparency index 70
- turn over 70

D

department

- administrators 53
- allow assignment 29
- approver 62-63
- approver (IT) 62-63
- assign company resources 25, 82
- assign devices 81, 168
- assign employees 81, 138
- assign extended properties 89
- assign workdesk 176
- assign workdesks 81
- attestors 53, 61, 63
- basics 11
- certification status 90
- conflicting roles 33, 87
- contact data 66
- country 66
- dynamic 85
- edit 63
- functional area 66
- IT operating data 76
- manager 63
- no inheritance 30-31, 63

- object ID 63
- profit 66
- risk index 66
- rule violation 66
- short name 63
- state 66
- transparency index 66
- turn over 66

device

- assign business role 163, 169
- assign company resources 167
- assign cost center 81, 163, 168
- assign department 81, 163, 168, 184
- assign location 81, 163, 168
- assign to workdesk 163, 179
- company 158
- device ID 163
- device model 155, 163
- device status 159, 184
- edit 161
- enter call 170
- location 184
- network configuration 165
- no inheritance 31, 163
- service agreement 170
- storage class 182, 184
- storage data 181
- storage type 182, 184
- workdesk 171

device model

- deactivate 156
- device type 156
- edit 155
- local periphery 156
- logic PC 156

- PC 156
- server 156
- device status 159
- device type 156
- direction of inheritance 11
- dynamic role
 - calculate 39, 44, 46-47
 - calculation schedule 36, 40, 50
 - condition 36, 50
 - test 38
 - cost center 85
 - department 85
 - edit excluded list 86
 - exclude employees 48, 86
 - excluded list 48
 - location 85
 - object class 50
 - organizations 50
 - recalculation 50
 - role 50
 - set up 36

E

- employee
 - access restriction 131
 - add to IT Shop 139
 - address 124
 - administrators 93
 - assign application role 140
 - assign business role 122, 139
 - assign company resources 133
 - assign cost center 81, 122, 138
 - assign department 81, 122, 138
 - assign extended properties 150
 - assign location 81, 138

- assign reports 142
- assign resource 141
- assign software 141
- assign system role 142
- assign to workdesk 119, 180
- central password 101, 125
- central SAP user account 125
- central user account 99, 125
- certification status 119, 132
- company 95, 119
- country 124, 148-149
- default email address 100, 125
- delete 130-131
- delete permissions 131
- deputy 122
- employee manager 93
- enter call 150
- entry date 122
- external 119
- identity 125
- identity card number 122
- image 124
- language 124, 148
- leaving date 122
- location 124
- locked 118
- log 118
- logins 125
- main identity 102, 125
- manager 122
- managerial scope 146
- new user 131
- no inheritance 31, 119
- permanently deactivate 119, 129
- phone 124

- pseudo employee 125
- reenable 129-130
- report 151
- risk index 119
- security key (Webauthn) 147
- security risk 119, 190
- state 124, 148-149
- subidentity 102
- system user 125
- temporarily deactivate 122, 128
- user account 146, 150
- work hours 149
- X500 person 125
- employee manager 93
- exclude list (dynamic role) 48
 - incorrect entries 86
- extended property 202
 - assign objects 208
 - assign property group 206
 - assign resource 196
 - assign to employee 150
 - create 204
 - overview form 207
 - property group 204
 - scope limit 204, 206

F

- functional area 59

G

- group identity 103

I

- identity
 - organizational 103
 - primary 103
- inheritance
 - block 30
 - bottom-up 11
 - calculate 20-22
 - halt 13, 30
 - limit 30-31
 - top-down 11
 - XIsInEffect 22
 - XOrigin 22
- inheritance exclusion 33
 - define for roles 87
- IT operating data 76
 - change 80

L

- leaser 95, 158
- location
 - address 74-75
 - administrators 53
 - allow assignment 29
 - approver 62, 72
 - approver (IT) 62, 72
 - assign company resources 25, 82
 - assign devices 81, 168
 - assign employees 81, 138
 - assign extended properties 89
 - assign workdesk 176
 - assign workdesks 81
 - attestors 53, 61, 72

- basics 11
- certification status 90
- conflicting roles 33, 87
- country 74
- dynamic 85
- edit 71
- functional area 75
- IT operating data 76
- manager 72
- network configuration 75
- no inheritance 30-31, 72
- profit 75
- risk index 75
- rule violation 75
- short name 72
- state 74
- transparency index 75
- turn over 75

M

- mail definition 97
- manufacturer 95, 158

O

- organizations
 - certify 90
- overview form
 - extended property 207
 - resource 195, 200

P

- password
 - central 101, 125

- password policy 105
 - assign 106
 - character sets 111
 - check password 116
 - conversion script 113, 115
 - default policy 106, 109
 - display name 109
 - edit 109
 - error message 109
 - excluded list 116
 - failed logins 110
 - generate password 117
 - initial password 110
 - name components 110
 - password age 110
 - password cycle 110
 - password length 110
 - password strength 110
 - predefined 105
 - test script 113
- property group 202
 - add 203
 - assign extended properties 205-206

R

- resource 187
 - assign extended properties 196
 - assign system role 195
 - assign to employee 141, 190
 - inheritance 190, 197
 - overview form 195, 200
 - requestable 190, 197
 - resource type 190, 197
 - risk index 190, 197
 - security risk 190

- service item 190, 197
 - set up 190
- resource type 190, 197
 - set up 189
- risk assessment
 - functional area 59
- risk index
 - for resource 190, 197
- role
 - conflicting roles 33
- role classes 56
 - role type 57, 59
- role type 57
 - assign 57, 59
 - create 58
 - role classes 57, 59
- roles
 - allow assignment 29
 - assign company resources 25
 - basics 11
 - inheritance
 - bottom-up 11
 - top-down 11
 - no inheritance 30-31

S

- service identity 103
- service item
 - for resource 190, 197
- software
 - assign to employee 141
 - assign to workdesks 178
- sponsored identity 103
- storage class 182
- storage type 182

- subscribable report
 - assign to employee 142
- supplier 95, 158
- system role
 - add resource 195
 - assign to employee 142
 - assign to workdesk 178
- system user 125
 - locked 118

T

- template
 - IT operating data, modify 80

U

- user account
 - apply template 80

W

- workdesk
 - assign business role 171, 177
 - assign company resources 174
 - assign cost center 81, 171, 176
 - assign department 81, 173, 176
 - assign device 179
 - assign employees 180
 - assign location 81, 173, 176
 - assign software 178
 - assign system role 178
 - create automatically 171
 - edit 171
 - no inheritance 31, 171
 - status 171
 - workdesk status 160

workdesk type 160, 171
workdesk status 160
workdesk type 160