



One Identity Manager 8.1.4

Identity Management Base Module Administration Guide

Copyright 2020 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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

One Identity Manager Identity Management Base Module Administration Guide
Updated - 19 October 2020, 07:41
Version - 8.1.4

Contents

Basics for mapping company structures in One Identity Manager	9
Hierarchical role structure basic principles	10
Inheritance directions within a hierarchy	10
Discontinuing inheritance	12
Basic principles for assigning company resources	14
Direct assignment	14
Indirect assignment	15
Secondary assignment	15
Primary assignment	16
Assignment by dynamic roles	17
Assigning through IT Shop requests	18
Basics of calculating inheritance	18
Calculating inheritance by hierarchical roles	19
Calculation of assignments	21
Preparing hierarchical roles for company resource assignments	22
Possible assignments of company resources through roles	23
Permitting assignments of employees, devices, workdesks, and company resources	25
Using roles to limit inheritance	26
Inheritance exclusion: Specifying conflicting roles	28
Managing departments, cost centers, and locations	30
One Identity Manager users for organizations	30
Basic data for structuring departments, cost centers, and locations	32
Role classes	33
Role types	34
Functional areas	34
Attestors	35
Role approvers and role approvers (IT)	36
Editing departments	38
General master data for a department	38
Contact data for departments	40
Functional area and risk assessment	41

Editing cost centers	42
General master data for a cost center	42
Functional area and risk assessment	44
Editing locations	46
General master data for a location	46
Location address information	48
Configuring a location's network	49
Directions to location	49
Functional area and risk assessment	50
Assigning employees, devices, and workdesks to departments, cost centers, and locations	51
Assigning company resources to departments, cost centers, and locations	52
Setting up IT operating data	54
Modify IT operating data	58
Additional tasks for managing departments, cost centers, and locations	59
Creating dynamic roles for departments, cost centers, and locations	59
Assign organizations	60
Specifying inheritance exclusion for roles	61
Reports about departments, cost centers, and locations	62
Working with dynamic roles	64
Editing dynamic roles	65
Dynamic role master data	66
Conditions for dynamic roles	67
Testing a condition of a dynamic role	67
Calculating role memberships	68
Additional tasks for dynamic roles	69
Dynamic role overview	69
Start immediate recalculation of role memberships	69
Employee administration	71
One Identity Manager users for employee administration	72
Basic data for employee master data	73
Business partners	74
Creating custom mail templates for notifications	75
General properties of a mail template	76
Creating and editing an email definition	78

Customizing email signatures	78
Entering employee master data	79
General employee master data	80
Organizational employee master data	82
Address data	84
Miscellaneous employee master data	85
Employee's central user account	88
Employee's central password	89
Employee's default email address	90
Mapping multiple employee identities	91
Employee identity types	92
Disabling and deleting employees	93
Temporarily deactivating employees	94
Permanently deactivating employees	94
Re-enabling an employee	95
Deferred deletion of employees	96
Deleting all employee related data	96
Password policies for employees	96
Predefined password policies	97
Using password policies	98
Changing the password policy for the password columns	99
Assigning password policies to departments, cost centers, locations, and business roles	99
Editing password policies	100
General master data for password policies	101
Policy settings	101
Character classes for passwords	103
Custom scripts for password requirements	104
Script for checking passwords	104
Script for generating a password	105
Defining the excluded list for passwords	106
Checking a password	107
Testing password generation	107
Informing employees about expiring passwords	107
Displaying locked employees and system users	108

Limited access to One Identity Manager	108
Changing the certification status of an employee	109
Assigning company resources to employees	110
Assigning employees to departments, cost centers, and locations	113
Assigning employees to business roles	114
Adding employees to IT Shop custom nodes	115
Assigning application roles to employees	116
Assigning resources directly to employees	116
Assigning software directly to employees	117
Assigning system roles directly to employees	117
Assigning subscribable reports directly to employees	118
Displaying the origin of an employee's roles and entitlements	118
Analyzing role memberships and employee assignments	120
Additional tasks for managing employees	122
Employee overview	122
Manually assigning user accounts to employees	122
Entering calls for an employee	123
Assigning extended properties	123
Displaying and deleting employees' Webauthn security keys	124
Setting a secret password question	124
Mutual aid	125
Determining an employee's language	126
Determining an employee's working hours	127
Employee reports	128
Managing devices and workdesks	130
Basic data for device admin	130
Device models	131
General master data for a device model	132
Inventory data for a device model	133
Business partners	134
Device status	135
Workdesk status	136
Workdesk types	136
Setting up a device	137
General master data for a device	139

Device networking data	141
Assigning company resources to devices	143
Assigning devices to departments, cost centers, and locations	144
Assigning devices to business roles	145
Additional tasks for managing devices	146
Overview of devices	146
Assigning service agreements and enter calls	146
How to set up workdesks	147
General master data for a workdesk	148
Workdesk location information	149
Additional information about a workdesk	150
Assigning company resources to workdesks	150
Assigning workdesks to departments, cost centers, and locations	152
Assigning workdesks to business roles	153
Assigning software directly to workdesks	154
Assigning system roles directly to workdesks	154
Additional tasks for managing workdesks	155
Workdesk overview	155
Assigning devices to workdesks	156
Assigning employees to workdesks	156
Asset data for devices	157
Basic data for asset management	157
Asset classes	157
Asset types	158
Entering investments and investment plans	158
Editing device asset data	159
Master data for asset data	159
Commercial data	161
Managing resources	163
One Identity Manager users for managing resources	164
Basic data for resources	165
Resource types	165
Editing resources	165
Resource master data	166
Assigning resources to employees	167

Assigning resources to departments, cost centers, and locations	167
Assigning resources to business roles	168
Assigning resources directly to employees	169
Adding resources to the IT Shop	169
Adding resources in system roles	170
Additional tasks for managing resources	171
Resource overview	171
Assigning extended properties to resources	171
Editing multi-request resources	172
Master data for a multi-request resource	173
Assigning multi-request resources to employees	174
Adding multi request resources to the IT Shop	174
Reports about resources	175
Setting up extended properties	176
One Identity Manager users for managing extended properties	176
Create property groups	177
Edit extended properties	178
Extended property master data	178
Specifying scoped boundaries	179
Additional tasks for managing extended properties	180
Extended property overview	180
Assign objects	180
Assigning property groups	181
Appendix: Configuration parameters for managing departments, cost centers, and locations	182
Appendix: Effective configuration parameters for setting up employees ...	184
Appendix: Configuration parameters for managing devices and workdesks	187
About us	189
Contacting us	189
Technical support resources	189
Index	190

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 detailed information on 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 edit permissions to the One Identity Manager objects to One Identity Manager users. For detailed information, see the *One Identity Manager Authorization and Authentication Guide*.

Detailed information about this topic

- [Hierarchical role structure basic principles](#) on page 10
- [Basic principles for assigning company resources](#) on page 14

- [Basics of calculating inheritance](#) on page 18
- [Preparing hierarchical roles for company resource assignments](#) on page 22

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 10
- [Discontinuing inheritance](#) on page 12

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**
Top-down inheritance maps the standard structure within a company in One Identity Manager. 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

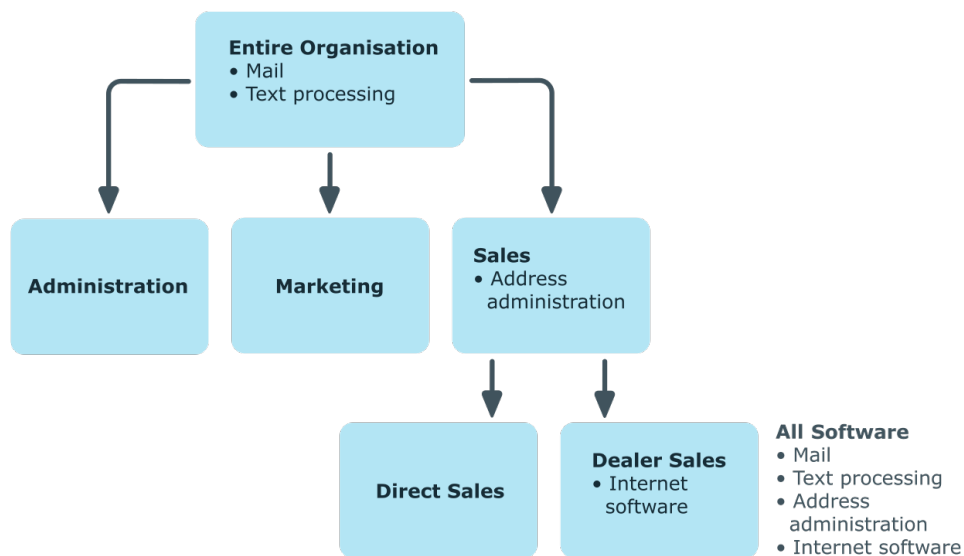
responsible for all child roles.

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

Example for assigning company resources top-down

In the diagram above a section of a company's structure is illustrated. In addition, system entitlements are listed that are assigned to the respective department. An employee in dealer sales is assigned all the system entitlements that are allocated to their department and all those on the entire organization path. In this case, these are the Azure Active Directory groups 1 and 2 and the SharePoint Online groups 1 and 2.

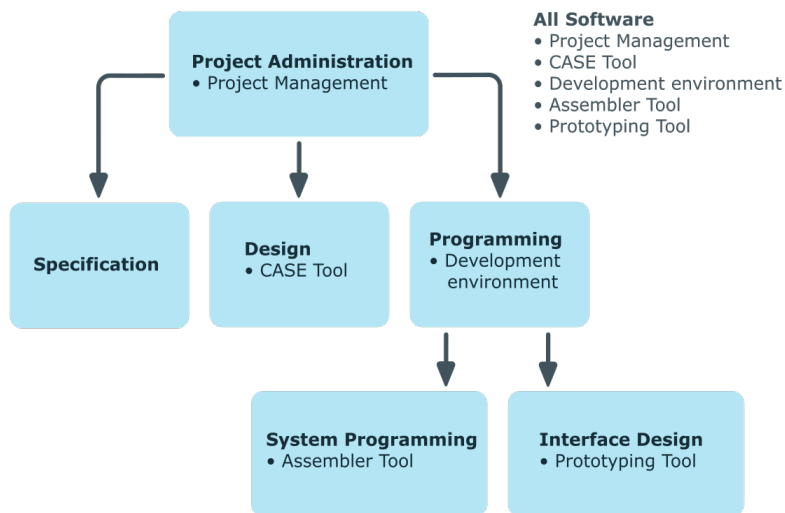
Figure 1: Assignment through top-down inheritance



Example for 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.

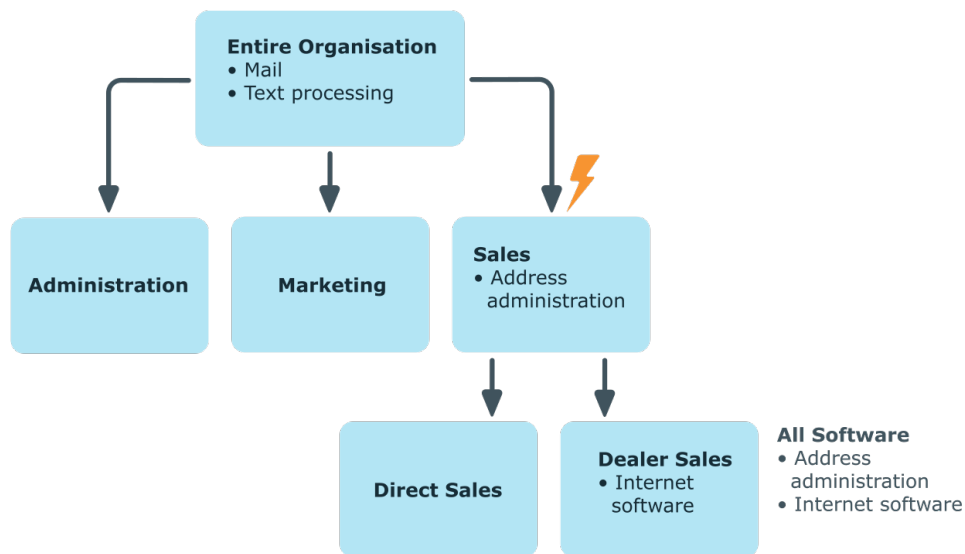
- Roles marked with the **Block inheritance** option do not inherit any assignments from parent levels in top-down inheritance. It can, however, pass on its own directly assigned company resources to lower level structures.
- In bottom-up inheritance, the role labeled with the "Block inheritance" option 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 for 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 SharePoint Online group 1 and employees in the "Dealer sales" department inherit the SharePoint Online groups 1 and 2. System entitlements of the "Entire organization" department are however, assigned to employees in the "Sales" and "Dealer sales" departments.

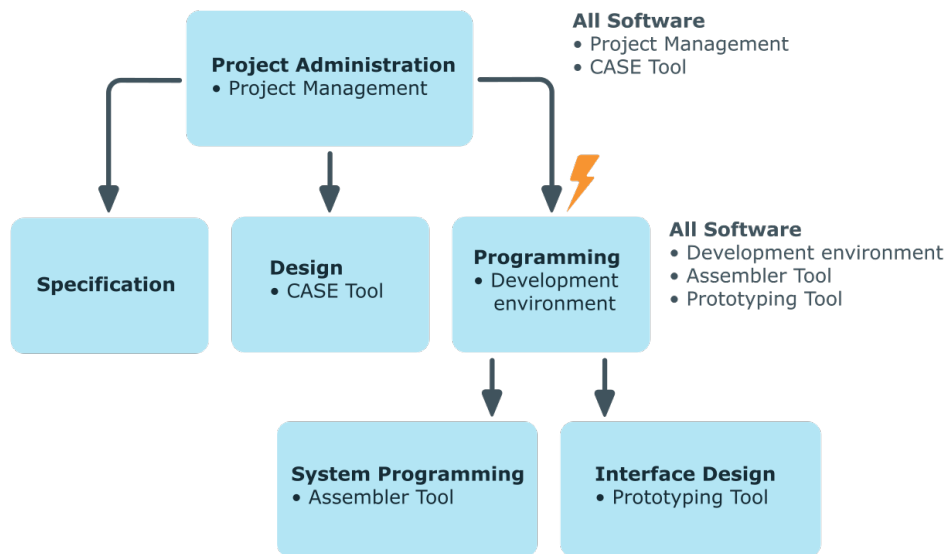
Figure 3: Discontinuing inheritance top-down



Example for 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



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 assignment](#)
- [Indirect assignment](#)
- [Assignment by dynamic roles](#)
- [Assigning through IT Shop requests](#)

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.

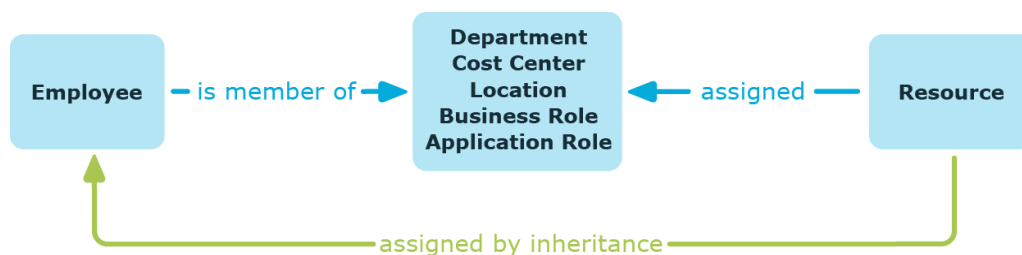
Figure 5: Schema of a direct assignment based on the example of an employee



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.

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



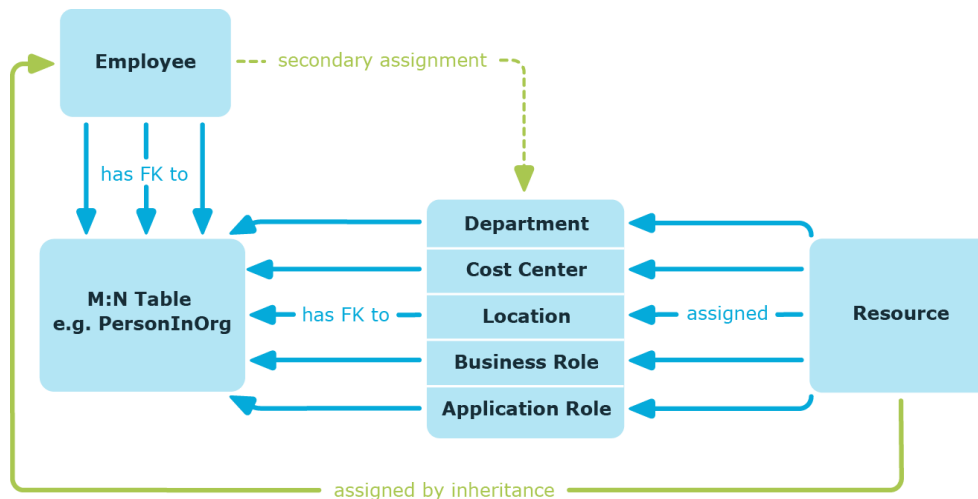
Related topics

- [Secondary assignment](#) on page 15
- [Primary assignment](#) on page 16

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



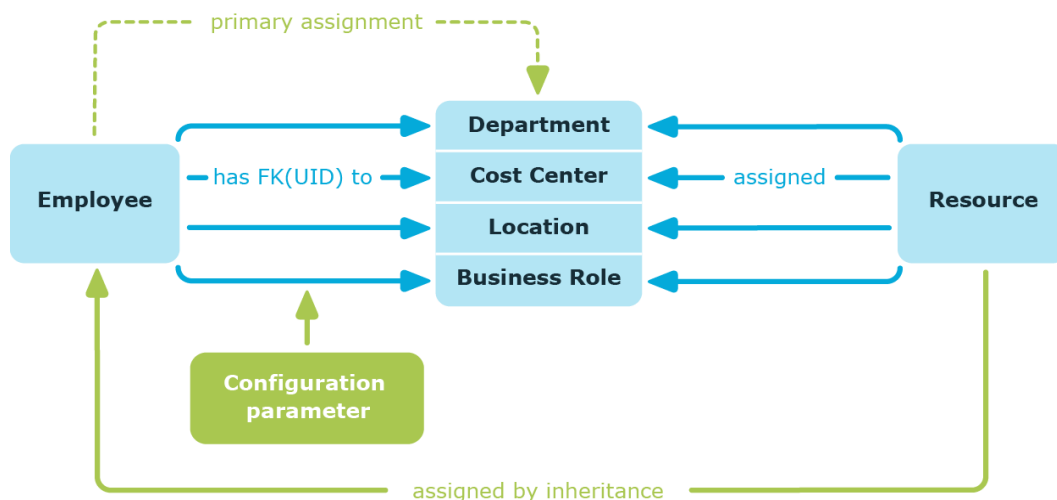
Related topics

- [Permitting assignments of employees, devices, workdesks, and company resources on page 25](#)

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 master 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 Workdesk FromDepartment	Workdesks inherit assignments from their primary 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).

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.

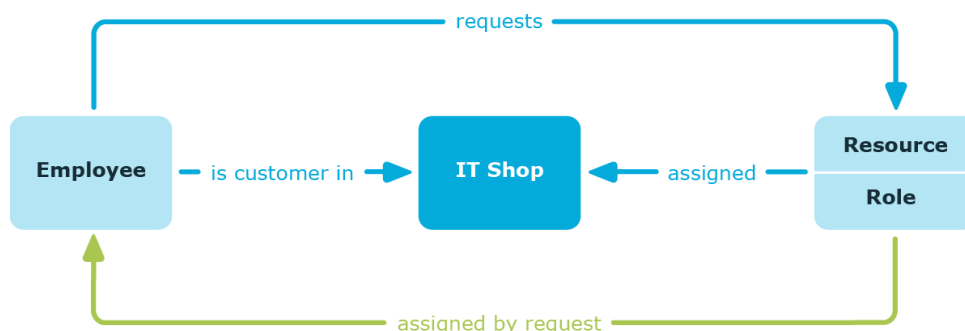
Related topics

- [Working with dynamic roles](#) on page 64

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.

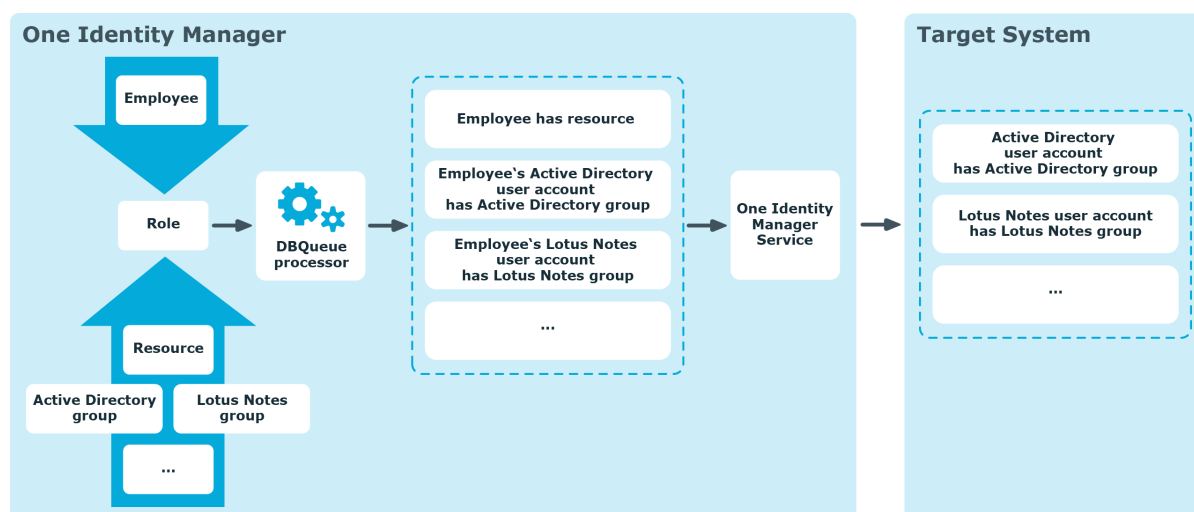
Figure 9: Schema of assignment by requests



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 19
- [Calculation of assignments](#) on page 21

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. The One Identity Manager data model contains 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:

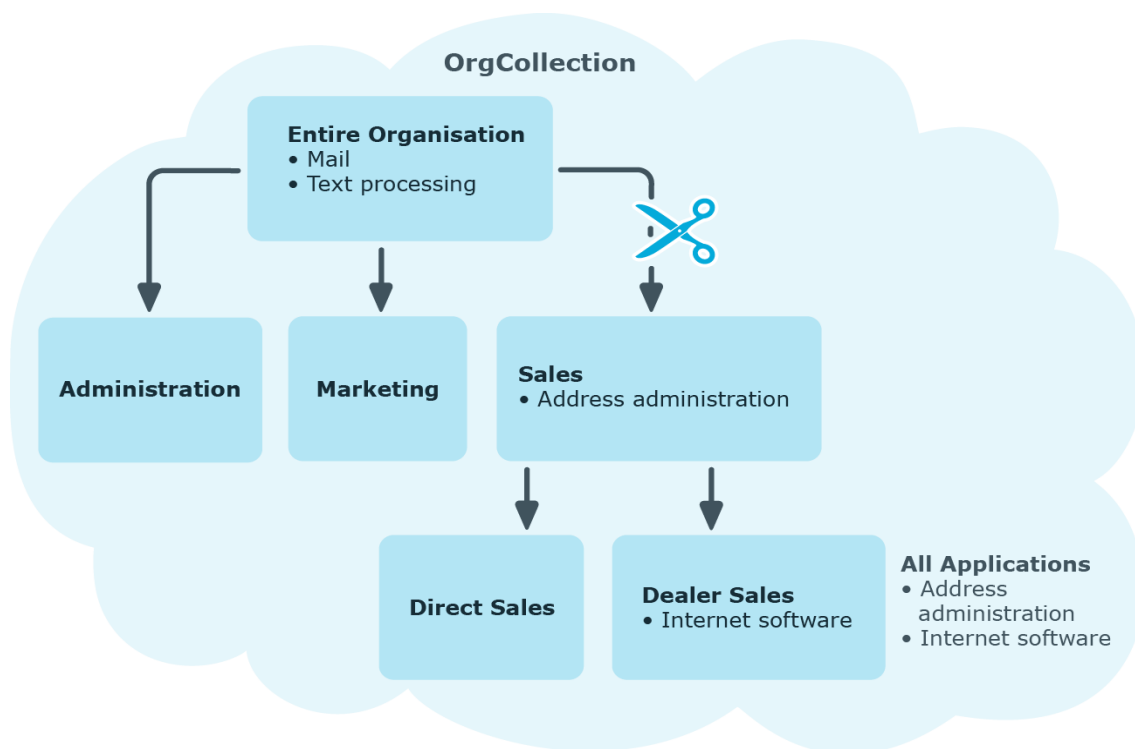
- UID_Org is the role that inherits.
- UID_ParentOrg is the role that passes down inheritance.

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 `XOrigin` 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 detailed information, see the administration guide of the module in which the bit is used.

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)

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`.

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.

Bit 3	Bit 2	Bit 1	Bit 0	Value in XOrigin	Meaning
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.

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.

- 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 necessary, define roles that are mutually exclusive.
You can prevent employees, devices, or workdesks being added to roles which contain mutually excluding company resources by specifying "conflicting roles".

Detailed information about this topic

- [Possible assignments of company resources through roles](#) on page 23
- [Permitting assignments of employees, devices, workdesks, and company resources](#) on page 25
- [Using roles to limit inheritance](#) on page 26
- [Inheritance exclusion: Specifying conflicting roles](#) on page 28

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	

Assignable Company Resource	Members in Roles	
	Employees	Workdesks
Groups of custom target systems	Possible (assigns to all an employee's custom defined target systems user accounts, for which group inheritance is authorized)	-
Active Directory groups	Possible (assigns to all an employee's Active Directory user accounts and Active Directory contacts, for which group inheritance is authorized)	-
SharePoint groups	Possible (assigns to all an employee's SharePoint user accounts)	-
SharePoint roles	Possible (assigns to all an employee's SharePoint user accounts)	-
LDAP groups	Possible (assigns to all an employee's LDAP user accounts for which group inheritance is authorized)	-
Notes groups	Possible (assigns to all an employee's Notes user accounts)	-
SAP groups	Possible (assigns to all an employee's SAP user accounts in the same SAP client.	-
SAP profiles	Possible (assigns to all an employee's SAP user accounts in the same SAP client.	-
SAP roles	Possible (assigns to all an employee's SAP user accounts in the same SAP client.	-
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 client.	-
BI analysis authorizations	Possible (assigns to all an employee's BI user accounts in the same system)	-
Azure Active Directory groups	Possible (assigns to all an employee's Azure Active Directory user accounts for which group inheritance is authorized)	-
Azure Active Directory administrator roles	Possible (assigns to all an employee's Azure Active Directory user accounts for which group inheritance is authorized)	-
Azure Active Directory subscriptions	Possible (assigns to all an employee's Azure Active Directory user accounts for which group inheritance is authorized)	-

Assignable Company Resource	Members in Roles	
	Employees	Workdesks
Disabled Azure Active Directory service plans	Possible (assigns to all an employee's Azure Active Directory user accounts for which group inheritance is authorized)	-
Unix groups	Possible (assigns to all an employee's Unix user accounts)	-
PAM user groups	Possible (assigns to all an employee's PAM user accounts for which 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 52

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

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 IT Shop, dynamic roles, or system roles.

Example

To assign employees in the Manager directly to a department, set the **Assignment allowed** and the **Direct assignment allowed** option on "department".

If employees can only obtain membership in a department through the IT Shop, set the **Assignment allowed** option but not the **Direct assignment allowed** option on the "department" role class for the entry "employees". 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.

To configure secondary assignment to roles of a role class

1. Select the role class under **Basic configuration data | Role classes**.
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.

Using roles to limit 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 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

1. Open the role's master data form.
2. Set the **Block inheritance** option.
3. Save the changes.

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 a role from inheriting

1. Open the role's master data form.
2. 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.
3. Save the changes.

Inheritance of company resources can be done in the same way 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. Open the employee's master data form.
2. 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.

3. Save the changes.

To prevent an device from inheriting

1. Open the device's master data form.
2. 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.

3. Save the changes.

To prevent a workdesk from inheriting

1. Open the workdesk's master data form.
2. 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.

3. Save the changes.

Related topics

- [Discontinuing inheritance](#) on page 12

Inheritance exclusion: Specifying conflicting roles

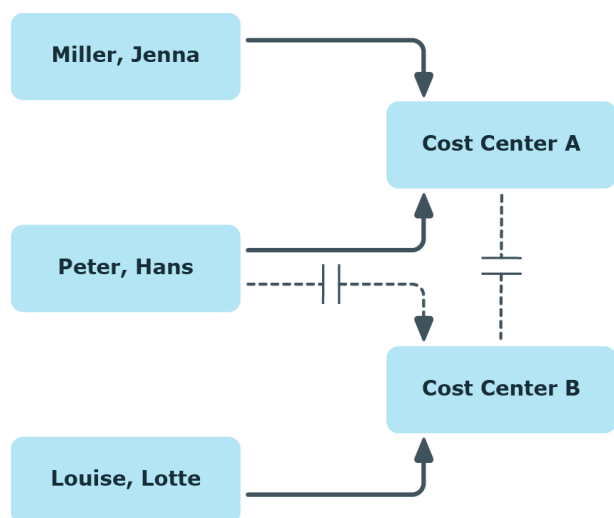
You can define conflicting roles to prevent employees, devices, or workdesks from being assigned to several roles at the same time and from obtaining mutually exclusive company resources through these roles. At the same time, you specify which application roles, departments, cost centers, and locations need to be 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. Jenna Miller and Hans Peters are members of cost center A. Louise Lotte is a member of cost center B. Hans Peters cannot be assigned to cost center B. Apart from that, One Identity Manager prevents Jenna Miller and Louise Lotte 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.

Related topics

- [Specifying inheritance exclusion for roles](#) on page 61

Managing 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, authorizations in different SAP systems or software. 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

- [Editing departments](#) on page 38
- [Editing cost centers](#) on page 42
- [Editing locations](#) on page 46
- [Setting up IT operating data](#) on page 54
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 51
- [Assigning company resources to departments, cost centers, and locations](#) on page 52
- [Preparing hierarchical roles for company resource assignments](#) on page 22

One Identity Manager users for organizations

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

Table 5: 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. • Administrate application roles for role approvers, role approvers (IT), and attestors. • Set up other application roles as required.
One Identity Manager administrators	<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.
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 master 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>
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.

User	Tasks
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.

Basic data for structuring departments, cost centers, and locations

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

- **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.
- **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.
- **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. A default application role for attestors is available in One Identity Manager. Assign employees that are authorized to attest permissions, requests, or other data stored in One Identity Manager to this application role. You may create other application roles as required. For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

- **Approvers and 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 approvers. Default application roles for approvers and approvers (IT) are available in One Identity Manager. Assign employees that are authorized to approve requests in the IT Shop to this application role. You may create other application roles as required. For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Detailed information about this topic

- [Role classes](#) on page 33
- [Role types](#) on page 34
- [Functional areas](#) on page 34
- [Attestors](#) on page 35
- [Role approvers and role approvers \(IT\)](#) on page 36
- [Configuration parameters for managing departments, cost centers, and locations](#) on page 182

Role classes

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 provided by default for mapping organizations in One Identity Manager:

- Department
- Cost center
- Location

The direction of inheritance is specified by the role class. Top down inheritance is defined for departments, cost centers, locations, and application roles. In addition, assignments that are allowed to be made to individual roles are defined for the role classes. 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 10
- [Permitting assignments of employees, devices, workdesks, and company resources](#) on page 25

Role types

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

To edit role types

1. Select the **Organizations | Basic configuration data | Role types** category.
2. Select the role type in the result list. Select the **Change master data** task.
 - OR -
 - Click  in the result list.
3. Edit the role type's master data.
4. Save the changes.

Enter the following master data for a role type:

Table 6: Role type properties

Property	Description
Role type	Role type description.
Description	Text field for additional explanation.

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 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.

Example for using functional areas are:

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 edit functional areas

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 master data** task.
- OR -
Click  in the result list.
3. Edit the function area master data.
4. Save the changes.

Enter the following data for a functional area.

Table 7: 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 in order to organize 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 input field is available if the Compliance Rules Module exists.
Description	Text field for additional explanation.

Related topics

- One Identity Manager Compliance Rules Administration Guide

Attestors

Installed modules: Attestation Module

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. A default application role for attestors is available in One Identity Manager. Assign employees that are authorized to attest permissions, requests, or other data stored in One Identity Manager to this application role. You may create other application roles as required. For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 8: 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 master 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 specify attestors

1. 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.

Related topics

- One Identity Manager Attestation Administration 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 approvers. Default application roles for approvers and approvers (IT) are available in One Identity Manager. Assign employees that are authorized to approve requests in the IT Shop to this application role. You may create other application roles as required. For detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 9: 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. Select the **Organizations | Basic configuration data | Approver** category.
- OR -
Select the **Organizations | Basic configuration data | Approver (IT)** category.
2. Select the **Assign employees** task.
3. In the **Add assignments** pane, assign employees.
- OR -
In the **Remove assignments** pane, remove employees.
4. Save the changes.

Related topics

- One Identity Manager IT Shop Administration Guide

Editing departments

To edit departments

1. Select the **Organizations | Departments** category.
2. Select a department in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the department's master data.
4. Save the changes.

Detailed information about this topic




- [General master data for a department](#) on page 38
- [Contact data for departments](#) on page 40
- [Functional area and risk assessment](#) on page 41
- [Setting up IT operating data](#) on page 54

General master data for a department

Enter the following data for a department.

Table 10: General master data for a department

Property	Description
Department	Name of the department
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 the menu. Leave this field empty if the department is at the top level of the department hierarchy.
Role type	Role types for more detailed classification.
Location	Location to which the department is primary assigned.
Default printer server	Printer server for the department. Select a server from the menu to assign it to the department.

Property	Description
	<p>NOTE: This property is only available if the Active Directory Module is installed.</p>
Manager	Manager responsible for the department.
2nd Manager	Assistant manager of the department.
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 – Department master data was granted approval by the manager. • Denied – Department master data was denied approval by the manager.
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.

Property	Description
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 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](#) on page 34
- [Attestors](#) on page 35
- [Role approvers and role approvers \(IT\)](#) on page 36
- [Using roles to limit inheritance](#) on page 26
- [Creating dynamic roles for departments, cost centers, and locations](#) on page 59

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 11: Contact data for departments

Property	Description
Email addresses	Email addresses for the department.

Property	Description
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

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

Table 12: Master 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 input field is only visible if the QER CalculateRiskIndex configuration parameter is set.
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	Specify how many rule violations are permitted for this department. The value can be evaluated when compliance rules are checked. 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 an employee's language](#) on page 126
- [Determining an employee's working hours](#) on page 127
- [Functional areas](#) on page 34
- One Identity Manager Risk Assessment Administration Guide
- One Identity Manager Compliance Rules Administration Guide

Editing cost centers

To edit a cost center

1. Select the **Organizations | Cost centers** category.
2. Select a cost center in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the data cost center's master data.
4. Save the changes.

Detailed information about this topic



- [General master data for a cost center](#) on page 42
- [Functional area and risk assessment](#) on page 44
- [Setting up IT operating data](#) on page 54

General master data for a cost center

Enter the following data for a cost center.

Table 13: General master data for a cost center

Property	Description
Cost center	Cost center name.
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

Property	Description
	the cost center hierarchy.
Role type	Role types for more detailed classification.
Manager	Manager responsible for the cost center.
2nd Manager	Deputy cost center manager.
Attestors	<p>Applications role whose members are authorized to approve attestation cases for this cost center.</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>
Department	Department to which the cost center is primary assigned.
Location	Location to which the cost center is primary assigned.
Role approver	<p>Application role whose members approve IT Shop requests for members of this cost center.</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 cost center.</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 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 – Cost center master data was granted approval by the manager • Denied – Cost center master data was denied approval by the manager.
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

Property	Description
	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.
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](#) on page 34
- [Attestors](#) on page 35
- [Role approvers and role approvers \(IT\)](#) on page 36
- [Using roles to limit inheritance](#) on page 26
- [Creating dynamic roles for departments, cost centers, and locations](#) on page 59

Functional area and risk assessment

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

Table 14: Master 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 input field is only visible if the QER CalculateRiskIndex configuration parameter is set.
Transparency index	Specifies how well you can trace cost center assignments. Use the slider to enter a value between 0 and 1. 0 ... no transparency 1 ... full transparency
Max. number of rule violations	Specify how many rule violations are permitted for this cost center. The value can be evaluated when compliance rules are checked. 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 an employee's language](#) on page 126
- [Determining an employee's working hours](#) on page 127
- [Functional areas](#) on page 34
- One Identity Manager Risk Assessment Administration Guide
- One Identity Manager Compliance Rules Administration Guide

Editing locations

To edit locations

1. Select the **Organizations | Locations** category.
2. Select a location in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the location's master data.
4. Save the changes.

Detailed information about this topic




- [General master data for a location](#) on page 46
- [Location address information](#) on page 48
- [Configuring a location's network](#) on page 49
- [Directions to location](#) on page 49
- [Functional area and risk assessment](#) on page 50
- [Setting up IT operating data](#) on page 54

General master data for a location

Enter the following data for a location.

Table 15: General master data for a location

Property	Description
Location	Name of the location.
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.
Role type	Role types for more detailed classification.
Manager	Manager responsible for the location.

Property	Description
2nd Manager	Assistant manager of the location.
Attestors	<p>Applications role whose members are authorized to approve attestation cases for this location.</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>
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	<p>Application role whose members approve IT Shop requests for members of this location.</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 location.</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 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 – Location master data was granted approval by the manager. • Denied – Location master data was denied approval by the manager.
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.

Property	Description
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. 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](#) on page 34
- [Attestors](#) on page 35
- [Role approvers and role approvers \(IT\)](#) on page 36
- [Using roles to limit inheritance](#) on page 26
- [Creating dynamic roles for departments, cost centers, and locations](#) on page 59

Location address information

Enter the following master data for contacting the location.

Table 16: Location's address data

Property	Description
Address	Postal address of the location.
Street	Street or road.
Building	Building

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

Related topics

- [Determining an employee's language](#) on page 126
- [Determining an employee's working hours](#) on page 127

Configuring a location's network

Enter the location's network configuration data.

Table 17: 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 18: Directions to location

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

Functional area and risk assessment

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

Table 19: Master 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 input field is only visible if the QER CalculateRiskIndex configuration parameter is set.
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	Specify how many rule violations are permitted for this location. The value can be evaluated when compliance rules are checked. 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](#) on page 34
- One Identity Manager Risk Assessment Administration Guide
- One Identity Manager Compliance Rules Administration Guide

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. Select the **Organizations | <Role class>** category.
2. Select the role in the result list.
3. Select the appropriate task.
 - Assign employees
 - Assign devices
 - Assign workdesk
4. In the **Add assignments** pane, assign objects.
- OR -
In the **Remove assignments** pane, remove objects.
5. Save the changes.

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

Related topics

- [Assigning company resources to departments, cost centers, and locations](#) on page 52
- [Creating dynamic roles for departments, cost centers, and locations](#) on page 59
- [Assigning employees to departments, cost centers, and locations](#) on page 113
- [Assigning devices to departments, cost centers, and locations](#) on page 144
- [Assigning workdesks to departments, cost centers, and locations](#) on page 152

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 by referencing a department, cost center, or location through a foreign key to the 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 20: Possible assignments of company resources to roles

Company Resource	Available in Module
Resources	always
Account definitions	Target System Base Module
Groups of custom target systems	Target System Base Module
Active Directory groups	Active Directory Module
SharePoint groups	SharePoint Module

Company Resource	Available in Module
SharePoint roles	SharePoint Module
LDAP groups	LDAP Module
Notes groups	IBM Notes Module
SAP groups	SAP R/3 User Management Module
SAP profiles	SAP R/3 User Management Module
SAP roles	SAP R/3 User Management Module
SAP parameters	SAP R/3 User Management 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
PAM user groups	Privileged Account Governance Module
G Suite groups	G Suite Module
G Suite products and SKUs	G Suite Module

To add company resources to a hierarchical role

1. Select **Organizations** | **<Role class>**.
 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.
- OR -

In the **Remove In the Add assignments pane, assign** pane, remove the company resources.

5. Save the changes.

Detailed information about this topic

- [Basic principles for assigning company resources](#) on page 14
- [Permitting assignments of employees, devices, workdesks, and company resources](#) on page 25

Related topics

- [Possible assignments of company resources through roles](#) on page 23
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 51
- [Working with dynamic roles](#) on page 64

Setting up IT operating data

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. Specify the "Department" property in the IT operating data formatting rule for the account definitions A and B 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.

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.

Table 21: IT operating data

Property	Description
Effects on	<p>IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.</p> <p>To specify an application scope</p> <ol style="list-style-type: none">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	<p>User account property for which the value is set.</p> <p>In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the <i>One Identity Manager Target System Base Module Administration Guide</i>.</p>
Value	Concrete value which is assigned to the user account property.

5. Save the changes.

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
IBM Notes	Server
	Certificate
	Template for mail file
	Identity
SharePoint	Authentication mode
	Groups can be inherited
	Identity
	Privileged user account
SharePoint Online	Groups can be inherited
	Privileged user account
	Authentication mode
Custom target systems	Container (per target system)
	Groups can be inherited
	Identity
	Privileged user account

Target system type	IT operating data
Azure Active Directory	Groups 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
Exchange Online	Groups can be inherited
Privileged Account Management	Authentication provider
	Identity
	Groups can be inherited
	Privileged user account
G Suite	Organization
	Identity
	Groups can be inherited
	Privileged user account
	Change password at next login

Related topics

- [One Identity Manager Target System Base Module Administration Guide](#)

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 executed.

To execute 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 **Execute 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.

Old value: Current value of the object property.

New value: Value that the object property would have following modification of the IT operating data.

Selection: Specifies whether or not the new value is transferred 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.

Additional tasks for managing departments, cost centers, and locations

After you have entered the master data, you can run the following tasks.

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. 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 master data.
5. Save the changes.

To edit a dynamic role

1. 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 master data** task.
6. Edit the dynamic role's master data.
7. Save the changes.

Related topics

- [Working with dynamic roles](#) on page 64
- [Editing dynamic roles](#) on page 65
- [General master data for a department](#) on page 38

- [General master data for a cost center](#) on page 42
- [General master data for a location](#) on page 46

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 master 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. 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 assigned to all departments as cost center or location.
- OR -
In the **Remove assignments** pane, remove the departments.
6. Save the changes.

To assign a department or a location to cost centers

1. 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 assigned to all cost centers as department or location.
- OR -
In the **Remove assignments** pane, remove the cost centers.
6. Save the changes.

To assign a department or a cost center to locations

1. 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 assigned to all locations as department or cost center.
- OR -
In the **Remove assignments** pane, remove the locations.
6. Save the changes.

Specifying inheritance exclusion for 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, you specify which application roles, departments, cost centers, and locations need to be 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.

To define inheritance exclusion for a departments

1. Select **Organizations | Departments** in the Manager.
2. Select the department in the result list.
3. Select the **Edit conflicting departments** task.
4. In **Add assignments**, assign the departments that are mutually exclusive to the selected department.
- OR -
In **Remove assignments**, remove the assignments that are no longer mutually exclusive.
5. Save the changes.

To define inheritance exclusion for a cost center

1. Select **Organizations | Cost centers** in the Manager.
2. Select the cost center in the result list.
3. Select the **Edit conflicting cost centers** task.

4. In **Add assignments**, assign the cost centers that are mutually exclusive to the selected cost center.
- OR -
In **Remove assignments**, remove the cost centers that are no longer mutually exclusive.
5. Save the changes.

To define inheritance exclusion for a cost center

1. Select **Organizations | Locations** in the Manager.
2. Select the location in the result list.
3. Select the **Edit conflicting locations** task.
4. In **Add assignments**, assign the locations that are mutually exclusive to the selected location.
- OR -
In **Remove assignments**, 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 28

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 23: 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.

Report	Description
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 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 .

Related topics

- [Analyzing role memberships and employee assignments](#) on page 120

Working with dynamic roles

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.

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.

Example of 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.

Detailed information about this topic

- [Editing dynamic roles](#) on page 65
- [Calculating role memberships](#) on page 68

Related topics

- [Basic principles for assigning company resources](#) on page 14
- [Permitting assignments of employees, devices, workdesks, and company resources](#) on page 25
- [Configuration parameters for managing departments, cost centers, and locations](#) on page 182

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. Select the role for which a dynamic role is to be created.
2. Select the **Create dynamic role** task.
3. Enter the required master data.
4. Save the changes.

To edit a dynamic role

1. 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 master data** task.
5. Edit the data and then save the changes.

Related topics

- [Creating dynamic roles for departments, cost centers, and locations](#) on page 59
- For detailed information about dynamic roles for application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Dynamic role master data

Enter the following data for a dynamic role.

Table 24: Dynamic role master 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. The Dynamic roles check schedule is already defined in the default One Identity Manager installation. All dynamic role memberships are checked using this schedule and recalculation requests are sent to the DBQueue Processor if necessary. Use the Designer to customize schedules or set up new ones to meet your requirements. For more detailed information, see the <i>One Identity Manager Operational Guide</i> .
Description	Text field for additional explanation.
Condition	Defines which objects of the object class become members of the selected role. For more information, see Conditions for dynamic roles on page 67.

For detailed information about using the WHERE clause wizard and the filter designer, see the *One Identity Manager User Guide for One Identity Manager Tools User Interface*.

Related topics

- [Editing dynamic roles](#) on page 65
- [Testing a condition of a dynamic role](#) on page 67
- [Start immediate recalculation of role memberships](#) on page 69

Conditions for dynamic roles

A dynamic role condition is defined as a valid where clause for database queries and must relate to the selected object class.

You can enter the conditions directly as a SQL query or use the Where clause wizard. Alternatively, you can enter conditions for employee objects with the filter designer.

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.

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.

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

Related topics


- [Testing a condition of a dynamic role](#) on page 67

Testing a condition of a dynamic role

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

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

To test the SQL condition

1. Select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select the form element "dynamic roles" and click on the dynamic role.
4. Select the **Change master data** task.
5. Click  (**Edit SQL**) on the form.
This displays the condition as SQL query.
6. Select the **Test condition** task.

On the master data form, in the **Test result** field, all objects determined by the condition are displayed.

Calculating role memberships

Table 25: Configuration parameters for calculating dynamic roles

Configuration parameter	Meaning
QER Structures DynamicGroupCheck	This 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 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.

In order to calculate role memberships, the 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

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

Tasks for recalculating memberships are set up depending on the configuration parameter settings by:

- Cyclical checking using a schedule

In the standard installation of One Identity Manager, the schedule **Dynamic roles check** is already defined. All dynamic role memberships are checked using this schedule and recalculation requests are sent to the DBQueue Processor if necessary.

Checks are made at predefined intervals. Use the Designer to customize schedules or set up new ones to meet your requirements. For more detailed information, see the *One Identity Manager Operational Guide*.

- Immediately an object has changed

Memberships are immediately checked by the DBQueue Processor and changed is necessary when object properties are changed. To use this function, in the Designer, set the **QER | Structures | DynamicGroupCheck | CalculateImmediatelyPerson**, **QER | Structures | DynamicGroupCheck | CalculateImmediatelyHardware**, and **QER | Structures | DynamicGroupCheck | CalculateImmediatelyWorkdesk** configuration parameters.

Related topics

- [Start immediate recalculation of role memberships](#) on page 69

Additional tasks for dynamic roles

After you have entered the master data, you can run the following tasks.

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. Select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select the form element "dynamic roles" and click on the dynamic role.
4. Select the **Dynamic role overview** task.

Start immediate recalculation of role memberships

By default, calculation of role membership is controlled with schedules. You can also start the calculation for a single dynamic role immediately and independently of scheduled calculation.

To calculate role membership immediately

1. Select the role for which the dynamic role was created.
2. Open the role's overview form.
3. Select the form element "dynamic roles" and click on the dynamic role.
4. Select the **Start recalculation immediately** task and close the prompt with **OK**.
A processing task for the DBQueue Processor is set in the DBQueue.

Detailed information about this topic

- [Calculating role memberships](#) on page 68

Employee administration

The main component of One Identity Manager maps employees with their master 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

- [Entering employee master data](#) on page 79
- [Disabling and deleting employees](#) on page 93
- [Assigning company resources to employees](#) on page 110
- [Displaying the origin of an employee's roles and entitlements](#) on page 118
- [Analyzing role memberships and employee assignments](#) on page 120
- [Mapping multiple employee identities](#) on page 91
- [Limited access to One Identity Manager](#) on page 108
- [Employee reports](#) on page 128

One Identity Manager users for employee administration

Following users are used for employee administration.

Table 26: Users

User	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 master data for all employees• Can assign a manager.• Can assign company resources to employees.• Check and authorize employee master data.• Create and edit risk index functions.• Edit password policies for employee passwords• Delete employee's security keys (WebAuthn)
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 master 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 master data of their staff.• Can add their staff members to the IT Shop.• Can view their staff's compliance rule violations in the Web Portal. <p>Members of this application role are determined through a dynamic role.</p>
One Identity Manager administrators	<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.

User	Tasks
	<ul style="list-style-type: none"> • Create custom processes in the Designer as required. • Create and configure schedules as required. • Create and configure password policies as required.

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

Basic data for employee master 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

- [Business partners](#) on page 74
- [Creating custom mail templates for notifications](#) on page 75
- [Password policies for employees](#) on page 96
- [Effective configuration parameters for setting up employees](#) on page 184

Business partners

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

To edit the data of a business partner

1. In the Manager, select the **Employees | Basic configuration data | Business partners** category.
2. Select a company in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the business partner's master data.
4. Save the changes.

Enter the following data for a company.

Table 27: General master data for a company

Property	Description
Company	Short description of the company for the views in One Identity Manager tools.
Name	Full company name.
Surname prefix	Additional company name.
Short name	Company's short name.
Contact	Contact person for the company.
Partner	Specifies whether this is a partner company.
Customer number	Customer number at the partner company.
Supplier	Specifies whether this is a supplier.
Customer number	Customers number at supplier.
Leasing partner	Specifies whether this is a leasing provider or rental firm.
Manufacturer	Specifies whether this is a manufacturer.
Remarks	Text field for additional explanation.

Table 28: 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 Browse button to display the web page in the default web browser.

Creating custom mail templates for notifications

A mail template consists of general master 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.

In One Identity Manager, there is a Mail Template Editor to simplify writing notifications. You can use the Mail Template Editor to create and edit mail texts in WYSIWYG mode.

To 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 master 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 master 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 master 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**.


Detailed information about this topic


- [Creating and editing an email definition](#) on page 78
- [Customizing email signatures](#) on page 78

General properties of a mail template

The following general properties are displayed for a mail template:

Table 29: Mail template properties


Property	Meaning
Mail template	Name of the mail template. This name will be used to display the mail templates in the administration tools and in the Web Portal. Translate the given text using the  button.

Property	Meaning
Base object	Mail template base object. A base object only needs to be entered if the mail definition properties of the base object are referenced.
Report (parameter set)	Report, made available through the mail template.
Description	Mail template description. Translate the given text using the  button.
Target format	Format in which to generate email notification. Permitted values are: <ul style="list-style-type: none"> • HTML: The email notification is formatted in HTML. Text formats, for example, different fonts, colored fonts, or other text formatting, can be included in HTML format. • TXT: The email notification is formatted as text. Text format does not support bold, italics, or colored font, or other text formatting. Images displayed directly in the message are not supported.
Design type	Design in which to generate the email notification. Permitted values are: <ul style="list-style-type: none"> • Mail template: The generated email notification contains the mail body in accordance with the mail definition. • Report: The generated email notification contains the report specified under Report (parameter set) as its mail body. • Mail template, report in attachment: The generated email notification contains the mail body in accordance with the mail definition. The report specified under Report (parameter set) is attached to the notification as a PDF file.
Importance	Importance for the email notification. Permitted values are Low , Normal , and High .
Confidentiality	Confidentiality for the email notification. Permitted values are Normal , Personal , Private , and Confidential .
Can unsubscribe	Specifies whether the recipient can unsubscribe email notification. If this option is set, the emails can be unsubscribed through the Web Portal.
Deactivated	Specifies whether this mail template is disabled.
Mail definition	Unique name for the mail definition.
Language	Language that applies to the mail template. The recipient's language preferences are taken into account when an email notification is generated.
Subject	Subject of the email message.
Mail body	Content of the email message.

Creating and editing an email definition

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. Open the mail template in the Mail Template Editor.
2. Click the  button next to the **Mail definition** list.
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 detailed 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. Open the mail template in the Mail Template Editor.
2. Select the language in **Mail definition**.
3. Edit the mail subject line and the body text.
4. Save the changes.

Using base object properties

In the subject line and body text of a mail definition, you can use all properties of the object entered under **Base object**. You can also use the object properties that are referenced by foreign key relation.

To access properties use dollar notation. For more detailed information, see the *One Identity Manager Configuration Guide*.

Customizing email signatures

Configure the email signature for mail templates using the following configuration parameter. Edit the configuration parameters in the Designer.

Table 30: Configuration parameters for email signatures

Configuration parameter	Description
Common MailNotification Signature	Data for the signature in email automatically generated from mail templates.

Configuration parameter	Description
Common MailNotification Signature Caption	Signature under the salutation.
Common MailNotification Signature Company	Company name.
Common MailNotification Signature Link	Link to the company's website.
Common MailNotification Signature LinkDisplay	Display text for the link to the company's website.

VI_GetRichMailSignature combines the components of an email signature according to the configuration parameters for use in mail templates.


Entering employee master data

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

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

- **Employees:** All activated and temporarily disabled employees.
- **Inactive employees:** All permanently disabled 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 edit employee master data

1. In the Manager, select the **Employees | Employees** category.
2. Select an employee in the result list and run the **Change master data** task.
– OR –
Click  in the result list.
This opens the master data form for an employee.
3. Edit the employee's master data.
4. Save the changes.

Ensure you fill out all compulsory fields when you edit the master data. Certain master 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 the One Identity Manager. Certain properties are locked due to being the master system. The source from which the employee master data is imported determines which properties are locked.

Detailed information about this topic

- [General employee master data](#) on page 80
- [Organizational employee master data](#) on page 82
- [Address data](#) on page 84
- [Miscellaneous employee master data](#) on page 85


General employee master data

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

Table 31: General master 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.
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.

Property	Description
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	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.
Certification status	<p>Specifies whether the employee master 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 master data has been approved by the manager. • Denied: The employee master data was not approved by the manager. The employee is permanently disabled.
VIP	Labels the employee as important.
Security risk	Specifies whether the employee is considered a risk for the company. Depending on how you configure this, you can prevent employees with such labels from inheriting resources and permissions and their user accounts are locked.
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	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.

Property	Description
Employee type	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 .
Contact email address	E-mail address to which the registration link is sent when a new user account is created using the Self-Registration Web Portal.
Company	Enter a company. Use the  next to the field to add a new company.
Workdesk	Employee's workdesk.
Risk index (calculated)	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 detailed information about risk assessment, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Description	Text field for additional explanation.
Comment	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

- [Changing the certification status of an employee](#) on page 109
- [Permanently deactivating employees](#) on page 94
- [Using roles to limit inheritance](#) on page 26
- [Business partners](#) on page 74
- [How to set up workdesks](#) on page 147

Organizational employee master data

Enter the following general master data for an organization.

Table 32: Organizational master data

Property	Description
Personnel	Employee's personnel number.

Property	Description
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.
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.
Temporarily disabled from	Date from which the employee and associated user accounts are disabled.

Property	Description
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	Change the date of the last working day if, for example, an employee leaves the company on a specific day but access to their data should be remain available for longer. 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 master data for their staff Certify employee master data for 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 22
- [Permanently deactivating employees](#) on page 94
- [Temporarily deactivating employees](#) on page 94

Address data

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

Table 33: 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

Property	Description
	determined though 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 can be 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 in the employee's data. 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 by the employee.
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 22
- [Determining an employee's language](#) on page 126
- [Determining an employee's working hours](#) on page 127

Miscellaneous employee master data

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

Table 34: Miscellaneous master 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 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 standard 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.
Default email address	Default email address for setting up the employee's inboxes in the individual target systems. This data is absolutely necessary for automatically creating mailboxes. In the One Identity Manager standard 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

Property	Description
	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.
Dummy employee	Specifies whether the employee represents an actual employee or a dummy employee, which is used, for example, for connecting to administrative user accounts.
Actual employee	Unique ID of the actual employee.
X500 dummy	Specifies whether the employee is managed as an X500 dummy in the One Identity Manager. If an employee has several X500 entries with different properties, you can also use a "Dummy" employee. Label the employee with the option X500 dummy in this case and configure a link to the real X500 employee.
X500 person	Assign the X500 dummy 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 detailed information about the One Identity Manager authentication modules, see the <i>One Identity Manager Authorization and Authentication Guide</i>.</p>
Starling 2FA user ID	User ID for multi-factor authentication. For detailed information about multi-factor authentication, see the <i>One Identity Manager IT Shop Administration Guide</i> .
System users	<p>System user with which the employee can log in to the One Identity Manager administration tools. The login data is analyzed by the authentication module in use.</p> <p>For detailed information about the One Identity Manager authentication modules, see the <i>One Identity Manager Authorization and Authentication Guide</i>.</p>
System user password and password confirmation	Employee's system user password. Password with which the employee logs in to the One Identity Manager tools.
User account name (mainframe)	If an employee is permitted access to the mainframe with their user account, enter the login name here.
Notebook	Just for information.

Property	Description
user	
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 into the network with their user account.
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 88
- [Employee's central password](#) on page 89
- [Employee's default email address](#) on page 90
- [Mapping multiple employee identities](#) on page 91
- [Employee identity types](#) on page 92

Employee's central user account

Table 35: Configuration parameter for forming the central user accounts

Configuration parameter	Meaning
QER Person CentralAccountGlobalUnique	<p>This configuration parameter 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>

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 36: Example of forming of central user accounts

First name	Last name	Central user account
Clara		CLARA
	Harris	HARRIS
Clara	Harris	CLARAH
Clara	Harrison	CLARAH1

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 use the central password of an employee for new user accounts belonging to the same employee, in the Designer, set the **QER | Person | UseCentralPassword | PermanentStore** configuration parameter.

If the configuration parameter is enabled, the central password is stored in the One Identity Manager database and is used for new users. If the configuration parameter is disabled, the central password is deleted from the One Identity Manager database following publishing to the existing user accounts. The central password is not available for new user accounts.

- 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 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 detailed information about changing 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 detailed information about editing scripts, see the *One Identity Manager Configuration Guide*.
- Use the Password Reset Portal to set the central password. For detailed information, see the *One Identity Manager Web Portal User Guide* and the *One Identity Manager Web Application Configuration Guide*.

Related topics

- [Miscellaneous employee master data](#) on page 85
- [Password policies for employees](#) on page 96
- [Setting a secret password question](#) on page 124
- [Mutual aid](#) on page 125
- [Displaying locked employees and system users](#) on page 108

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 88

Mapping multiple employee identities

Table 37: Configuration parameter for representing multiple identities

Configuration parameter	Effect when set
Person MasterIdentity UseMasterForAuthentication	<p>This configuration parameter specifies whether the main identity should be used to log in to One Identity Manager tools through an employee-linked authentication module.</p> <p>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.</p> <p>For detailed information about the One Identity Manager authentication modules and about editing system users, see the <i>One Identity Manager Authorization and Authentication Guide</i>.</p>

It may be necessary for employees to have different identities for their work under certain circumstances – for example, identities that result from contracts at different branches. These identities can be differentiated through the membership of a department, cost center or through access permissions. 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 master data for 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 master data for 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 master 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 92

Employee identity types

To differentiate the different identities of a person, use the following identity types.

Table 38: 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 the Organizational identity type. Also enter a main identity.
Personalized admin identity	Virtual person (sub-identity) that belongs to a user account of the Personalized administrator identity type.

Value	Description
	Also enter a main identity.
Sponsored identity	Dummy employee who is linked to a user account of the Sponsored identity type. Assign a manager to the employee.
Shared identity	Dummy employee who is linked to an administrative user account of the Shared identity type. Assign a manager to the employee.
Service identity	Dummy employee who is linked to a user account of the Service identity type. Assign a manager to the employee.
Machine identity	Dummy employee for mapping machine identities.

The primary identity, the organizational identity, and the personal admin identity are different identities under which the same actual person can execute 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 Entitlements to the different user accounts.

The sponsored identity, group identity, and service identity are dummy persons through which the connected user accounts are given permissions for the relevant target systems. The classification of dummy 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 dummy persons. In the evaluation of reports, attestations, or compliance checks, you check whether dummy employees need to be handled in a specific way.

Related topics

- [Miscellaneous employee master data](#) on page 85
- [Mapping multiple employee identities](#) on page 91

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.

The following methods are available in the One Identity Manager standard version:

- [Temporarily deactivating employees](#)
- [Permanently deactivating employees](#)
- [Deferred deletion of employees](#)

Temporarily deactivating employees

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 94
- [Deferred deletion of employees](#) on page 96

Permanently deactivating employees

Employees can be disabled 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 disabling of an employee 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 **Disable employee permanently** task
This task ensures that the **Permanently disabled** option is enabled and that the leaving date and the date of the last working day are set to the current date.
- Arrival of the leaving date
NOTE: Check the **Lock accounts of employees** that have left the company schedule in the Designer. This schedule regularly checks the leaving date and sets the **Permanently disabled** option on reaching the date.
NOTE: 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** through attestation or manually, the employee is permanently disabled with immediate effect. 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 94
- [Deferred deletion of employees](#) on page 96
- [Re-enabling an employee](#) on page 95
- [Changing the certification status of an employee](#) on page 109

Re-enabling an employee

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

To re-enable an employee

1. In the Manager, select the **Employees | Inactive employees** category.
2. Select the employee in the result list.
3. Select the **Re-enable employee** task.
4. Confirm the security prompt with **Yes** if the employee should be enabled.
On the master data form for the employee, the **Disabled permanently** 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 94

Deferred deletion of employees

When an employee is deleted, they are tested to see if user accounts and company resources are still assigned, or if there are still pending requests in the IT Shop. The employee is marked for deletion and therefore locked out of further processing. 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 one employee could 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.

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.

Related topics

- [Temporarily deactivating employees](#) on page 94
- [Permanently deactivating employees](#) on page 94

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: During execution of this procedure, the database does not allow any triggers. Therefore, it is recommended to only run the procedure in maintenance periods.

You can execute 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>'
```

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 97
- [Using password policies](#) on page 98
- [Editing password policies](#) on page 100
- [Custom scripts for password requirements](#) on page 104
- [Defining the excluded list for passwords](#) on page 106
- [Checking a password](#) on page 107
- [Testing password generation](#) on page 107
- [Informing employees about expiring passwords](#) on page 107

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

Related topics

- [Employee's central password](#) on page 89

Using 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 97
- [Changing the password policy for the password columns](#) on page 99
- [Assigning password policies to departments, cost centers, locations, and business roles](#) on page 99

Changing the password policy for the 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 | 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 access code, 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 | Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.

- Click **Add** in **Assignments** and enter the following data.

Table 39: Assigning a password policy

Property	Description
Apply to	<p>Application scope of the password policy.</p> <p>To specify an application scope</p> <ol style="list-style-type: none">Click ➔ next to the field.Under Table, select the table that contains the basic objects. You have the following options:<ul style="list-style-type: none">Departments (Department table)Business roles (Org table)<p>NOTE: This table is only available if the Business Roles Module is installed.</p><ul style="list-style-type: none">Locations (Locality table)Cost centers (Profitcenter table)Under Apply to, select the specific department, cost center, location, or business role.Click OK.
Password column	<p>The password column's identifier. You have the following options:</p> <ul style="list-style-type: none">Employees - central password (Employee table, CentralPassword column)Employees - password (Employee table, DialogUserPassword column)Employees - access code (Employee table, Passcode column)
Password policy	<p>The identifier of the password policy to be used.</p>

- Save the changes.

Editing password policies

To edit a password policy

- In the Manager, select the **Employees | Basic configuration data | Password policies | Password policies** category.
- Select the password policy in the result list and select **Change master data**.
- Edit the password policy's master data.
- Save the changes.




Detailed information about this topic

- [General master data for password policies](#) on page 101
- [Policy settings](#) on page 101
- [Character classes for passwords](#) on page 103
- [Custom scripts for password requirements](#) on page 104

General master data for password policies

Enter the following master data for a password policy.

Table 40: Master 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.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. 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.

Policy settings

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

Table 41: 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.

Property	Meaning
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is 256 .
Max. errors	<p>Maximum number of errors. Set the number of invalid passwords attempts. Only taken into account when logging in to One Identity Manager.</p> <p>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 reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager.</p> <p>You can use the Password Reset Portal to reset the passwords of employees and system users who have been blocked. For more detailed information, see the <i>One Identity Manager Web Portal User Guide</i>.</p>
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
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.
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 detailed 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 42: Character classes for passwords

Property	Meaning
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 or not a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether or not a generated password can contain uppercase letters. This setting only applies when passwords are generated.

Property	Meaning
Do not generate digits	Specifies whether or not a generated password can contain digits. This setting only applies when passwords are generated.
Do not generate special characters	Specifies whether or not 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

- [Script for checking passwords](#) on page 104
- [Script for generating a password](#) on page 105

Script for checking passwords

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 of a 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| Password policies** category.
 - b. In the result list, select the password policy.
 - c. Select the **Change master 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

- [Script for generating a password](#) on page 105

Script for generating a password

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 for a script to generate a password

The script replaces the ? and ! characters at the beginning of random passwords 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| Password policies** category.
 - b. In the result list, select the password policy.
 - c. Select the **Change master 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

- [Script for checking passwords](#) on page 104

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 | Restricted passwords** 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 a password

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

To check if a password conforms to the password policy

1. In the Manager, select the **Employees | Basic configuration data | Password policies | Password policies** category.
2. Select the password policy in the result list.
3. Select the **Change master 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.

Testing password generation

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 | Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change master 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 employees 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 detailed information about the 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 reached the number of maximum failed logins, the employee or system user can no longer 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 locked in Password Reset Portal. This unlocks the employees and system users again. For detailed information, see the *One Identity Manager Web Portal User Guide* and the *One Identity Manager Web Application Configuration Guide*.

Related topics

- [Employee's central password](#) on page 89

Limited access to One Identity Manager

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

User who only has temporary or limited access to Web Portal can log in through the One Identity Manager. 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**
 - **Disabled permanently: Enabled**
 - **No inheritance: Enabled**
- 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 editing permissions in One Identity Manager, implement custom processes.

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

Related topics

- [Changing the certification status of an employee](#) on page 109

Changing the certification status of an employee

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

Employee's certification status is set by default through certification and recertification procedures. For more detailed 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. In the Manager, select the **Employees | Employees** category to change the certification status of an active employee.
 - OR -

In the Manager, select the **Employees | Inactive employees** category to change the certification status of a permanently disabled employee.

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 disabled** 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 permanently disabled. If the employee's certification status is changed to **Certified**, the employee is enabled again.

Related topics

- [Limited access to One Identity Manager](#) on page 108
- [Permanently deactivating employees](#) on page 94

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. The 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 43: 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 are added to the associated application group, which permit application inheritance.
Active Directory groups	-	+	All the employee's Active Directory user accounts and Active Directory contacts are added to Active Directory groups, which permit group inheritance.
SharePoint groups	-	+	All the employee's SharePoint user accounts are added to SharePoint groups.
SharePoint roles	-	+	All the employee's SharePoint user accounts are added to SharePoint roles.
LDAP groups	-	+	All the employee's LDAP user accounts, which permit group inheritance, are added to LDAP groups.
Notes groups	-	+	All the employee's Notes user accounts are

Company Resource	Direct assignment permitted	Indirect assignment permitted	Comment
			added to Notes groups.
SAP groups	+	+	All the employee's SAP user accounts, which are in the same SAP clients, are added to SAP groups.
SAP profiles	+	+	All the employee's SAP user accounts, which are in the same SAP clients, are added to SAP profiles.
SAP roles	+	+	All the employee's SAP user accounts, which are in the same SAP clients, are added to SAP roles.
Structural profiles	-	+	All the employee's SAP user accounts, which are in the same SAP clients, are added to structural profiles.
BI analysis authorizations	-	+	All the employee's BI user accounts, which are in the same system, obtain BI analysis authorizations.
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 added to E-Business Suite groups.
Azure Active Directory groups	-	+	All the employee's Azure Active Directory user accounts, which permit group inheritance, are added to Azure Active Directory groups.
Azure Active Directory administrator roles	-	+	All the employee's Azure Active Directory user accounts, which permit group inheritance, are added to Azure Active Directory administrator roles.
Azure Active Directory subscriptions	-	+	All the employee's Azure Active Directory user accounts, which permit group inheritance, are given Azure Active Directory subscriptions.
Disabled Azure Active Directory service plans	-	+	All the employee's Azure Active Directory user accounts, which permit group inheritance, are given Azure Active Directory service plans.

Company Resource	Direct assignment permitted	Indirect assignment permitted	Comment
Unix groups	-	+	All the employee's Unix user accounts, which permit group inheritance, are added to Unix groups.
PAM user groups	-	+	All the employee's PAM user accounts for which the inheritance of groups is permitted are added to the PAM user groups.

Detailed information about this topic

- [Basic principles for assigning company resources](#) on page 14
- [Permitting assignments of employees, devices, workdesks, and company resources](#) on page 25

Related topics

- [Possible assignments of company resources through roles](#) on page 23
- [Assigning employees to departments, cost centers, and locations](#) on page 113
- [Assigning employees to business roles](#) on page 114
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 51
- [Assigning company resources to departments, cost centers, and locations](#) on page 52
- [Working with dynamic roles](#) on page 64

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 master data** task.
4. Adjust the following master 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 110
- [Assigning company resources to departments, cost centers, and locations](#) on page 52
- [Working with dynamic roles](#) on page 64
- [Adding employees to IT Shop custom nodes](#) on page 115
- [Assigning employees to business roles](#) on page 114
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 51

Assigning employees to business roles

NOTE: This function is only available if the module 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 detailed information about working with business roles, see *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, 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 master 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 110

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

Assigned employees obtain all the write 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.

Employees of the parent application role are inherited if no employees are directly assigned to an application role.

NOTE: The application roles for **Base roles | Everyone (Change)**, **Base roles | Everyone (Lookup)**, **Base roles | Employee Managers**, and **Base roles | Birthright 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.
 - OR -
 - In the **Remove assignments** pane, remove the application roles.
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.
 - OR -
 - In the **Remove assignments** pane, remove resources.
5. Save the changes.

Related topics

- [Assigning resources directly to employees](#) on page 169
- [Managing resources](#) on page 163

Assigning software directly to employees

NOTE: This function is only available if the module 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 detailed 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.
- OR -
In the **Remove assignments** pane, remove software.
5. Save the changes.

Assigning system roles directly to employees

NOTE: This function is only available if the module 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 detailed 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 assigned system roles.

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 module 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 detailed 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 an employee's 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

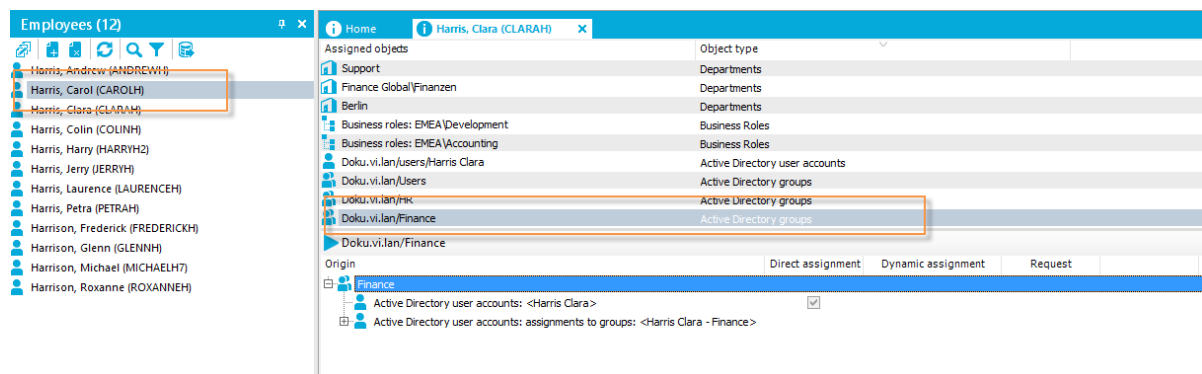
- In the Designer, set the **SysConfig | Display | SourceDetective** configuration parameter and compile the database.

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 of entitlement origin

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

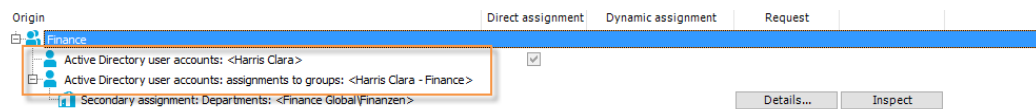


The report answers several questions.

Question Why does Clara Harris have the Active Directory group?

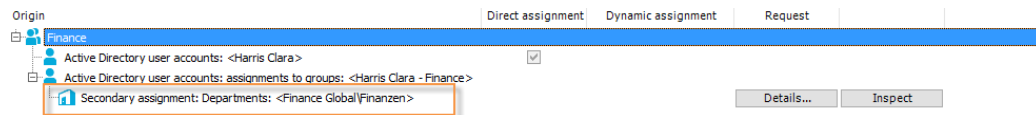
Answer Clara Harris owns an Active Directory user account and this user account is

assigned to the "Finance" group.

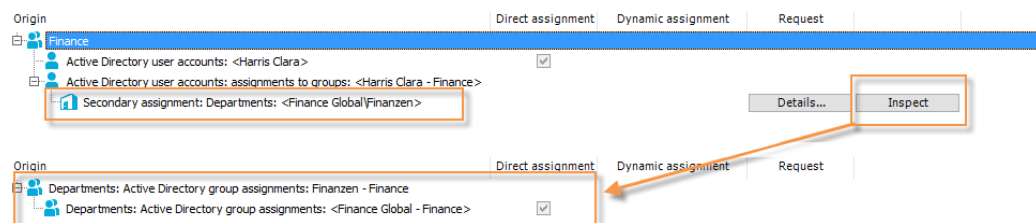


Question Why is the user account assigned to the "Finance" group?

Answer Clara Harris is assigned to the department "Finance" department.

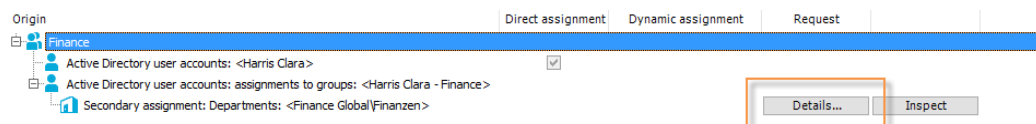


The "Finance" department inherits from the "Global Finance" department. The "Global Finance" department is directly assigned to the "Finance" group.



Question Why is Clara Harris in the "Finance" department?

Answer There is a department membership request for Clara Harris.




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.

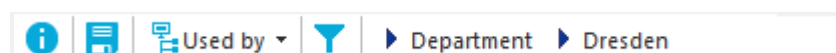






Table 44: Meaning of icons in the report toolbar

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.

Additional tasks for managing employees

After you have entered the master data, you can run the following tasks.

Employee 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.

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 detailed information about account definitions, see the *One Identity Manager Target System Base Module Administration Guide*.

To enable a quick response 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

- [Employee overview](#) on page 122

Entering calls for an employee

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

Enter the calls for employees through the Helpdesk Module. For detailed 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


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

- [Edit extended properties](#) on page 178

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 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.

Setting a secret password question

If you forget your password, you can change this at any time in the Password Reset Portal. To do this, you need to define individual questions that only you can answer.

You define the password questions in the Web Portal. For more detailed information, see the *One Identity Manager Web Portal User Guide*.

In exceptional cases, you can also define password questions in the Manager.

To enter your password questions

1. In the Manager, open your own employee data.
2. Select the **Change security question** task.
3. On the **Edit password questions** form, click **Add** and enter the following

information:

- **Query for password:** Enter your question.
 - **Reply for password:** Enter the answer to your (above) question.
4. Repeat the steps above for the remaining password questions.
 5. Click **OK**.

Related topics

- [Mutual aid](#) on page 125

Mutual aid

To change your passwords, you use the Password Reset Portal. For more detailed information, see the *One Identity Manager Web Portal User Guide*.

In exception cases, a person can use mutual aid in the Manager to reset their central password and their system user password. To do this, the password questions must be answered.

To grant mutual aid

1. In the Manager, open your own employee data.
2. Select the **Mutual aid - set password** task.

The employee for whom you want to grant mutual aid can change their central password and their system user password on this form.

To change the central password

1. Enter your central user account under **Login name**.
2. Enter your personnel number.
3. Click **Next**.
The password questions are displayed.
4. Enter the answers to your password questions in the input fields.
5. Click **Enable**.
6. In the **Central password** field, enter a new password.
7. In the **Confirmation** field, enter the password again.
8. Click **Save**.

To change your system user password

1. Enter your central user account under **Login name**.
2. Enter your personnel number.

3. Click **Next**.
The password questions are displayed.
4. Enter the answers to your password questions in the input fields.
5. Click **Enable**.
6. In the **System user password** field, enter a new password.
7. In the **Confirmation** field, enter the password again.
8. Click **Save**.

Related topics

- [Setting a secret password question](#) on page 124

Determining an employee's language

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 detailed 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 an employee's 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 detailed 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 of the primary location to the primary department, the primary cost center, 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 USA

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 45: 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, extended, or canceled.</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. Show... shows you the current approval status of pending requests.</p>
Data quality of supervised employees	This report evaluates the data quality of employee data records. All employees under supervision are taken into account.
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 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	The report contains different analyzes of data quality for all employees. You can find this report in My One Identity Manager .

report	Description
--------	-------------

for
employee
records

Related topics

- [Displaying the origin of an employee's roles and entitlements on page 118](#)
- [Analyzing role memberships and employee assignments on page 120](#)

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.

Detailed information about this topic

- [Basic data for device admin](#) on page 130
- [Setting up a device](#) on page 137
- [How to set up workdesks](#) on page 147
- [Asset data for devices](#) on page 157

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 Model

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 the manufacturer and supplier companies for 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 Type

Provide workdesk types for further classification of workdesks.


Detailed information about this topic

- [Device models](#) on page 131
- [Business partners](#) on page 134
- [Device status](#) on page 135
- [Workdesk status](#) on page 136
- [Workdesk types](#) on page 136
- [Configuration parameters for managing devices and workdesks](#) on page 187

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 edit a device model

1. Select the **Devices & Workdesks | Basic configuration data | Device models** category.
2. Select a device model in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the device model's master data.
4. Save the changes.



Detailed information about this topic

- [General master data for a device model](#) on page 132
- [Inventory data for a device model](#) on page 133

General master data for a device model

Enter the following general master data for a device model.

Table 46: Device model master 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 master data.
Company	Name of manufacturer. Use the  next to the field to add a new company. For more information, see Business partners on page 134. 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. Use the Browse task to see the manufacturer's website in the standard 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 a device model

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 comma can be modified as required.

Table 47: Inventory data for a device model


Property	Description
Default supplier	Name of supplier. For more information, see Business partners on page 134.
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.
Last quote date	Last quote date.

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

Business partners

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

To edit the data of a business partner

1. Select the **Devices & Workdesks | Basic configuration data | Business partners** category.
2. Select a company in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the business partner's master data.
4. Save the changes.

Enter the following data for a company.

Table 48: General master data for a company

Property	Description
Company	Short description of the company for the views in One Identity Manager tools.
Name	Full company name.
Surname prefix	Additional company name.
Short name	Company's short name.
Contact	Contact person for the company.
Partner	Specifies whether this is a partner company.
Customer number	Customer number at the partner company.
Supplier	Specifies whether this is a supplier.
Customer number	Customers number at supplier.

Property	Description
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 49: 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 Browse button to display the web page in the default web browser.

Device status

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

To edit a device status

1. Select the **Devices & Workdesks | Basic configuration data | Device status** category.
2. Select a device status in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the device's master data.
4. Save the changes.

Enter the following data for a device status.


Table 50: 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.

Workdesk status

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

To edit a workdesk status

1. Select the **Devices & Workdesks | Basic configuration data | Workdesk status** category.
2. Select the workdesk status in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the workdesk status's master data.
4. Save the changes.

Enter the following data for a workdesk status.

Table 51: Master data for a workdesk


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

Workdesk types

Provide workdesk types for further classification of workdesks, Enter additional device prerequisites are diskettes or CD drives necessary, for example.

To edit a workdesk type

1. Select the **Devices & Workdesks | Basic configuration data | Workdesk type** category.

2. Select the workdesk type in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the workdesk type's master data.
4. Save the changes.

Enter the following data for a workdesk type.

Table 52: Master data for a workdesk type

Property	Description
Workdesk type	Workdesk status name.
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.

Setting up a device

Table 53: 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 workstation and server 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 edit a device

1. Select the **Devices & Workdesks | Devices** category.
2. Select one of the following nodes.
 - Personal computer
 - Server
 - Monitors
 - Mobile phones
 - Tablets
 - Printers
 - Miscellaneous

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

3. Select a device in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
4. Edit the device's master data.
5. Save the changes.

Detailed information about this topic

- [General master data for a device](#) on page 139
- [Device networking data](#) on page 141
- [Asset data for devices](#) on page 157
- [Assigning company resources to devices](#) on page 143

General master data for a device

Enter the following general master data for a device. The master data available depends on the selected device model.

Table 54: General master data for a device

Property	Description
Asset number	Number of the asset in the bookkeeping.
Device ID	Unique device ID.
PC	Specifies whether the hardware is a computer.
Server	Specifies whether the hardware is a server.
Local peripheral	Specifies whether this is a local peripheral, for example, monitor, printer, or other peripheral device.
Manufacturer	Name of manufacturer.
Device model	Name of the device model. The master 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 activated, 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 hardware is host for a virtual machine.
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.

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

- [Device models](#) on page 131
- [Business partners](#) on page 134
- [Device status](#) on page 135
- [Asset data for devices](#) on page 157
- [Entering investments and investment plans](#) on page 158
- [How to set up workdesks](#) on page 147
- [Basic principles for assigning company resources](#) on page 14
- [Using roles to limit inheritance](#) on page 26

Device networking data

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

Table 55: Network data

Property	Description
IP	IP address in IPv4 format.

Property	Description
address (IPv4)	
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 DNS 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. The 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 the One Identity Manager modules and are not available until the modules are installed.

Table 56: 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 14
- [Permitting assignments of employees, devices, workdesks, and company resources](#) on page 25

Related topics

- [Possible assignments of company resources through roles](#) on page 23
- [Assigning devices to departments, cost centers, and locations](#) on page 144
- [Assigning devices to business roles](#)
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 51
- [Assigning company resources to departments, cost centers, and locations](#) on page 52
- [Assigning company resources to workdesks](#) on page 150
- [Working with dynamic roles](#) on page 64

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. 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. Select the **Device & Workdesks | Basic configuration data | <filter>** category.
2. Select the device in the result list.
3. Select the **Change master data** task.
4. Adjust the following master data:
 - Primary department
 - Primary cost center
 - Primary location
5. Save the changes.

Related topics

- [Assigning company resources to devices](#) on page 143
- [Assigning company resources to departments, cost centers, and locations](#) on page 52
- [Working with dynamic roles](#) on page 64
- [Assigning employees to business roles](#) on page 114
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 51

Assigning devices to business roles

Installed modules: Business Roles Module


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.

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

1. Select the **Devices & Workdesks | <filter>** category.
2. Select the device in the result list.
3. Select the **Assign business roles** task.
4. In the **Add assignments** pane, 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. Select the **Devices & Workdesks | <filter>** category.
2. Select the device in the result list.
3. Select the **Change master data** task.
4. Enter the primary role.
5. Save the changes.

Related topics

- [Assigning company resources to devices](#) on page 143
- One Identity Manager Business Roles Administration Guide

Additional tasks for managing devices

After you have entered the master data, you can run the following tasks.

Overview of devices

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

To obtain an overview of a device

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

Assigning service agreements and enter calls

Installed modules: Helpdesk Module

Use the Helpdesk Module to enter service agreements and calls for a device.

To enter help desk data for a device

1. 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.

Detailed information about this topic

- One Identity Manager Help Desk Module User Guide

How to set up workdesks


Table 57: Configuration parameters for setting up workdesk

Configuration parameter	Effect when set
Hardware Workdesk WorkdeskAuto	When workstation or server is setup an associated workdesk is created automatically.

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 edit a workdesk

1. Select the **Devices & Workdesks | Workdesks | Names** category.
2. Select a workdesk in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the workdesk's master data.
4. Save the changes.

Detailed information about this topic

- [General master data for a workdesk](#) on page 148
- [Workdesk location information](#) on page 149
- [Additional information about a workdesk](#) on page 150
- [Assigning company resources to workdesks](#) on page 150
- [Configuration parameters for managing devices and workdesks](#) on page 187

General master data for a workdesk

Enter the following general master data for a workdesk.

Table 58: General master data for a workdesk

Property	Description
Workdesk	Workdesk name. 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.
Operating system	Workdesk's operating system.
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.

Property	Description
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 corresponding to 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

- [Workdesk types](#) on page 136
- [Workdesk status](#) on page 136
- [Basic principles for assigning company resources](#) on page 14
- [Using roles to limit inheritance](#) on page 26

Workdesk location information

Enter the following information about a workdesk's location.

Table 59: 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.

Property	Description
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 14

Additional information about a workdesk

Enter additional device prerequisites are diskettes or CD drives necessary, for example.

Table 60: 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. The 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 workdesks.

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

Table 61: 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 14
- [Permitting assignments of employees, devices, workdesks, and company resources](#) on page 25

Related topics

- [Possible assignments of company resources through roles](#) on page 23
- [Assigning workdesks to departments, cost centers, and locations](#) on page 152
- [Assigning workdesks to business roles](#)
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 51
- [Assigning company resources to departments, cost centers, and locations](#) on page 52
- [Working with dynamic roles](#) on page 64

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. 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. Select the **Devices & Workdesks | Workdesks | Names** category.
2. Select the workdesk in the result list.
3. Select the **Change master data** task.

4. Adjust the following master data:

- Primary department
- Primary cost center
- Primary location

5. Save the changes.

Related topics

- [Assigning company resources to workdesks](#) on page 150
- [Assigning company resources to departments, cost centers, and locations](#) on page 52
- [Working with dynamic roles](#) on page 64
- [Assigning devices to business roles](#) on page 145
- [Assigning employees, devices, and workdesks to departments, cost centers, and locations](#) on page 51

Assigning workdesks to business roles

Installed modules: Business Roles Module


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.

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

1. 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, 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. Select the **Devices & Workdesks | Workdesks | Names** category.
2. Select the workdesk in the result list.
3. Select the **Change master data** task.

4. Enter the primary role.
5. Save the changes.

Related topics

- [Assigning company resources to workdesks](#) on page 150
- One Identity Manager Business Roles Administration Guide

Assigning software directly to workdesks

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, cost centers, locations, or business roles.

To react quickly to special requests, you can assign software directly to a workdesk. Information about the software is written to the workstation set up file that is assigned to this workdesk.

To assign software to a workdesk

1. Select the **Devices & Workdesks | Workdesks | Names** category.
2. Select the workdesk in the result list.
3. Select the **Assign software** task to assign software directly to the workdesk.
4. In the **Add assignments** pane, assign the software.
 - OR -
 - In the **Remove assignments** pane, remove the software.
5. Save the changes.

Related topics

- [Assigning workdesks to departments, cost centers, and locations](#) on page 152
- [Assigning workdesks to business roles](#) on page 153

Assigning system roles directly to workdesks

Installed modules: System Roles Module

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.


To react quickly to special requests, you can assign system roles directly to a workdesk.

To assign system roles to a workdesk

1. 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 assigned system roles.

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 152
- [Assigning workdesks to business roles](#) on page 153
- One Identity Manager System Roles Administration Guide

Additional tasks for managing workdesks

After you have entered the master data, you can run the following tasks.

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. 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 master data.

To assign devices to a workdesk

1. 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.
 - OR -
 - In the **Remove assignments** pane, remove the devices.
5. Save the changes.

Related topics

- [General master data for a device](#) on page 139

Assigning employees to workdesks

Use this task to assign a workdesk to several employees. You can also assign the workdesk through the employee's master data. By assigning a workdesk to an employee, all the user accounts for this employee are assigned as default PC to the associated workstation. This assignment is required for finding application licenses.

To assign employees to a workdesk

1. 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, assign employees.
 - OR -
 - In the **Remove assignments** pane, remove employees.
5. Save the changes.

Related topics

- [General employee master data](#) on page 80

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.

Detailed information about this topic

- [Basic data for asset management](#) on page 157
- [Entering investments and investment plans](#) on page 158
- [Editing device asset data](#) on page 159

Basic data for asset management

The following basic data is available for asset management.

- Asset classes
Enter the possible asset classes for asset data about devices.
- Asset types
Enter the possible asset types for asset data about devices.


Detailed information about this topic

- [Asset classes](#) on page 157
- [Asset types](#) on page 158
- [Basic data for device admin](#) on page 130
- [Configuration parameters for managing devices and workdesks](#) on page 187

Asset classes

Enter asset classes for asset data about a device.

To edit an asset class

1. Select the **Devices & Workdesks | Basic configuration data | Asset classes** category.
2. Select the asset class in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the asset class's master data.
4. Save the changes.

Enter the following data for an asset class.


Table 62: Asset class master 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.

Asset types

Enter asset types for asset data about a device.

To edit an asset type

1. Select the **Devices & Workdesks | Basic configuration data | Asset types** category.
2. Select an asset type in the result list. Select the **Change master 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

Enter the data for investments and investment plans and assign them to devices.

To edit an investment

1. Select the **Devices & Workdesks | Investments** category.
2. Select an investment in the result list. Select the **Change master data** task.

- OR -

Click  in the result list.

3. Edit the following master data.

Table 63: Master data for investments

Property	Description
Investment	Investment project name.
Date	Investment date.
Investment manager	The employee responsible for this investment.
Description	Text field for additional explanation.
Remarks	Text field for additional explanation.

4. Save the changes.

Related topics

- [General master data for a device](#) on page 139

Editing device asset data

To enter asset information for a device

1. Select the **Devices & Workdesks | <filter>** category.
2. Select the device in the result list.
3. Select the **Edit asset data** task.
4. Save the changes.

Detailed information about this topic

- [Master data for asset data](#) on page 159
- [Commercial data](#) on page 161

Master data for asset data

Enter the following master data for the asset data of a device.

Table 64: 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 or not 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.
Serial number	Serial number of the device.
Delivery remarks	Text field for additional explanation.
Inventory remarks	Text field for additional explanation.
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

- [Asset classes](#) on page 157
- [Asset types](#) on page 158
- [Basic principles for assigning company resources](#) on page 14

Commercial data

Enter the following asset data for a device.

NOTE: Prices are given to 2 decimal places by default. The number of commas can be modified in the Designer.

Table 65: Device asset data

Property	Description
Acquisition date	Date of purchase.
Delivery date	Date of delivery.
Delivery voucher number	Delivery voucher number.
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.
Leasing fee	Leasing fee.
Internal transfer price	Internal transfer price.
Depreciation month	Depreciation in months

Related topics

- [Business partners](#) on page [134](#)

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 66: Resource types

Type	Description	Table
Resources	Resources that an employee (workstation, 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 canceled. 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 longer needed. The resources are assigned to the employees after approval has been granted. They remain assigned until the request is canceled.	QERRReuseUS

Type	Description	Table
	Example: printer, monitor.	

Detailed information about this topic

- [Editing resources](#) on page 165
- [Assigning resources to employees](#) on page 167
- [Editing multi-request resources](#) on page 172
- [Assigning multi-request resources to employees](#) on page 174
- [Reports about resources](#) on page 175

One Identity Manager users for managing resources

The following users are used for user administration.

Table 67: Users

User	Tasks
Administrators for the IT Shop	<p>Administrators must be assigned to the Request & Fulfillment IT Shop Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Edit the resources and assign them to IT Shop structures and employees.
One Identity Manager administrators	<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 165
- [Edit extended properties](#) on page 178

Resource types


You can use resource types to group resources.

To define resource types

1. Select the **Entitlements | Basic configuration data | Resource types** category.
2. Select a resource type in the result list. Select the **Change master data** task.
– OR –
Click  in the result list.
3. Enter a name and description for the resource type.
4. Save the changes.

Editing resources

To edit resources

1. Select the **Entitlements | Resources** category.
2. Select a resource in the result list. Select the **Change master data** task.
– OR –
Click  in the result list.
3. Edit the resource's master data.
4. Save the changes.

Detailed information about this topic

- [Resource master data](#) on page 166
- [Assigning resources to employees](#) on page 167

Resource master data

Enter the following master data for a resource.

Table 68: Resource master 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 automatically requested or assigned with it.
Risk index	Value for evaluating the risk of resource assignments to employees. Enter a value between 0 and 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set.
IT Shop	Specifies whether the resource can be requested through the IT Shop. The resource can be ordered by an employee over the Web Portal and distributed using a defined approval process. The resource can also be assigned directly to employees and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the resource can only be requested through the IT Shop. The resource can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the resource cannot be directly assigned to roles outside the IT Shop.
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 assigned automatically to all internal employees. The resource is assigned to every employee not marked as external, on saving. New employees automatically obtain this resource as soon as they are added.</p> <p>Disable this option to remove automatic assignment of the resource</p>

Property	Description
	to all employees. The resource cannot be reassigned to employees from this point on. Existing resource 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

- [Resource types](#) on page 165
- One Identity Manager Risk Assessment Administration Guide
- One Identity Manager IT Shop Administration Guide

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.

Prerequisites for indirect assignment of resources to employees are:

- 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](#) on page 25
- [Basic principles for assigning company resources](#) on page 14

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. 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

- [Managing departments, cost centers, and locations](#) on page 30
- [Basics for mapping company structures in One Identity Manager](#) on page 9

Assigning resources to business roles

Installed modules: Business Roles Module


Assign a resource to business roles such that the resource is inherited by employees through these business roles.

To assign a resource to business roles

1. 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, 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.

Detailed information about this topic

- One Identity Manager Business Roles Administration Guide

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. 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 71
- [Basic principles for assigning company resources](#) on page 14

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.

To add a resource to the IT Shop

1. 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. 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. 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 with this resource are canceled in the process.

Related topics

- [Resource master data](#) on page 166
- One Identity Manager IT Shop Administration Guide

Adding resources in system roles

Installed modules: System Roles Module

A resource can be added to different system roles. A system role that is only contains resources can be labeled with "Resource package". 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.

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. 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.
- OR -
In the **Remove assignments** pane, remove system roles.
5. Save the changes.

Detailed information about this topic

- One Identity Manager System Roles Administration Guide

Additional tasks for managing resources

After you have entered the master data, you can run the following tasks.

Resource 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. 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. Select the **Entitlements | Resources** category.
2. Select a resource in the result list.
3. Select the **Assign extended properties** task.
4. In the **Add assignments** pane, assign extended properties.
- OR -
In the **Remove assignments** pane, remove extended properties.
5. Save the changes.

Detailed information about this topic


- [Edit extended properties](#) on page 178

Editing multi-request resources


You can only edit multi-request resources if the **QER | ITShop** configuration parameter is enabled.

- In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.

To edit multi-request resources

1. Select the **Entitlements | Multi-request resources for IT Shop** category.
2. Select a resource in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the multi-request resource's master data.
4. Save the changes.

To edit multi-requestable/unsubscribable resources

1. Select the **Entitlements | Multi requestable/unsubscribable resources for IT Shop** category.
2. Select a resource in the result list. Select the **Change master data** task.
- OR -
Click  in the result list.
3. Edit the multi-requestable/unsubscribable resource's master data.
4. Save the changes.

Detailed information about this topic

- [Master data for a multi-request resource](#) on page 173
- [Assigning multi-request resources to employees](#) on page 174

Master data for a multi-request resource

Enter the following master data for a multi-request resource.

Table 69: Master 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.
Risk index	Value for evaluating the risk of resource assignments to employees. Enter a value between 0 and 1. This input field is only visible if the QER CalculateRiskIndex configuration parameter is set.
IT Shop	Specifies whether the resource can be requested through the IT Shop. The resource can be ordered by an employee over the Web Portal and distributed using a defined approval process. The resource can also be assigned directly to employees and roles outside the IT Shop. This option cannot be disabled.
Only for use in IT Shop	Specifies whether the resource can only be requested through the IT Shop. The resource can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the resource cannot be directly assigned to roles outside the IT Shop. This option cannot be disabled.
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 165
- One Identity Manager IT Shop Administration Guide
- One Identity Manager Risk Assessment Administration Guide

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.

Detailed information about this topic

- [Assigning through IT Shop requests](#) on page 18
- One Identity Manager IT Shop Administration Guide

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.

Adding multi-request resources to the IT Shop

1. Select the **Entitlements | Multi-request resources for IT Shop** category.
- OR -
Select the **Entitlements | Multi requestable/unsubscribable resources for IT Shop** 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 multi request resources from individual IT Shop shelves

1. Select the **Entitlements | Multi-request resources for IT Shop** category.
- OR -

Select the **Entitlements | Multi requestable/unsubscribable resources for IT Shop** 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 multi-request resources from all IT Shop shelves

1. Select the **Entitlements | Multi-request resources for IT Shop** category.
- OR -

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.

Detailed information about this topic

- One Identity Manager IT Shop Administration Guide

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 70: 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 120

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

- [Create property groups](#) on page 177
- [Edit extended properties](#) on page 178

One Identity Manager users for managing extended properties

The following users are used for managing extended properties.

Table 71: Users


User	Tasks
Administrators for the IT Shop	Administrators must be assigned to the Request & Fulfillment IT Shop Administrators application role. Users with this application role:

User	Tasks
	<ul style="list-style-type: none"> • Create extended properties for company resources of any type.
One Identity Manager administrators	<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.

Create property groups

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.

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.

Edit 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 master data** task.
 - OR -
 - Click  in the result list.
3. Edit the extended property's master data.
4. Save the changes.

Detailed information about this topic

- [Extended property master data](#) on page 178
- [Specifying scoped boundaries](#) on page 179

Extended property master data

Enter the following data for an extended property.

Table 72: Extended property master data

Property	Description
Extended property name	Name of the extended property.
Property group	<p>The property group for structuring extended properties. You can assign a primary property group to a property on the master data form. Extended properties are grouped by this property group in navigation.</p> <p>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.</p>
Lower scope boundary	Lower scope boundary for further subdivision.

Property	Description
Upper scope boundary	Upper scope boundary for further subdivision.
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.

Detailed information about this topic

- [Specifying scoped boundaries](#) on page 179

Specifying scoped boundaries

You can subdivide extended properties by specifying scoped boundaries. You are not obliged to enter scoped boundaries. 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 boundaries:

- Basically, any string is permitted as a lower or upper scoped boundary.
- 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.

Additional tasks for managing extended properties

After you have entered the master data, you can run the following tasks.

Extended property 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.

Assign objects

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. Select the desired object type in the **Select object type** menu.
The object belonging to the object types are displayed on the form.
5. In the **Add assignments** pane, assign objects.

- OR -

In the **Remove assignments** pane, remove objects.

6. Save the changes.

Assigning 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.

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.

- OR -

In the **Remove assignments** pane, remove property groups.

5. Save the changes.

Related topics

- [Create property groups](#) on page 177

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 73: Configuration parameter

Configuration parameter	Description
QER Structures	If the configuration parameter is set, hierarchical roles are supported.
QER Structures DynamicGroupCheck	This 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 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

Configuration parameter	Description
	parameter is set, mutually excluding roles can be defined. Changes to this parameter require the database to be recompiled.
QER Structures Inherit Employee	This configuration parameter specifies whether employees can inherit through primary assignments.
QER Structures Inherit Employee GroupExclusion	This configuration parameter specifies whether employees inherit assignments from their primary department (Person.UID_Department).
QER Structures Inherit Employee FromLocality	This configuration parameter specifies whether employees inherit assignments from their primary location(Person.UID_Locality).
QER Structures Inherit Employee FromProfitCenter	This configuration parameter specifies whether employees inherit assignments from their primary cost center(Person.UID_ProfitCenter).
QER Structures Inherit Hardware	This configuration parameter specifies whether devices inherit through primary assignment.
QER Structures Inherit Hardware FromDepartment	This configuration parameter specifies whether devices inherit assignments from their primary department (Hardware.UID_Department).
QER Structures Inherit Hardware FromLocality	This configuration parameter specifies whether devices inherit assignments from their primary location (Hardware.UID_Locality).
QER Structures Inherit Hardware FromProfitCenter	This configuration parameter specifies whether devices inherit assignments from their primary cost center (Hardware.UID_ProfitCenter).
QER Structures Inherit Workdesk	This configuration parameter specifies whether workdesks can inherit through primary assignments.
QER Structures Inherit Workdesk FromDepartment	This configuration parameter specifies whether workdesks inherit assignments from their primary department (Workdesk.UID_Department).
QER Structures Inherit Workdesk FromLocality	This configuration parameter specifies whether workdesks inherit assignments from their primary location (Workdesk.UID_Locality).
QER Structures Inherit Workdesk FromProfitCenter	This configuration parameter specifies whether workdesks inherit assignments from their primary cost center (Person.UID_ProfitCenter).

Effective configuration parameters for setting up employees

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 74: Configuration parameter

Configuration parameter	Description
QER Person	If this configuration parameter is set, employee administration is supported.
QER Person CentralAccountGlobalUnique	<p>This configuration parameter 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	This configuration parameter contains the default mail domain. The value is used to establish an employee's email address.
Person MasterIdentity UseMasterForAuthentication	<p>This configuration parameter specifies whether the main identity should be used to log in to One Identity Manager tools through an employee linked authentication module.</p> <p>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.</p>
QER Person PasswordResetAuthenticator InvalidateUsedQuery	This configuration parameter defines whether the password questions user for a successful password reset become invalid after they are used.

Configuration parameter	Description
QER Person PasswordResetAuthenticator QueryAnswerDefinitions	This configuration parameter determines the number of password questions that an employee has to define in order to change their password.
QER Person PasswordResetAuthenticator QueryAnswerRequests	This configuration parameter determines the number of password questions that an employee has to answer in order to change their password.
QER Person PasswordResetAuthenticator PasscodeSplit	This parameter determines whether an access code generated by the helpdesk is split into two components, one for the helpdesk and one for the employee's manager.
QER Person TemporaryDeactivation	<p>This configuration parameter controls the behavior between employees and user accounts if employees are temporarily inactivated.</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	This configuration parameter 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	This configuration parameter specifies if 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 PermanentStore	This configuration parameter controls the storage period for central passwords. If the configuration parameter is enabled, the central password is stored in the One Identity Manager database and is used for new users. If the configuration parameter is disabled, the central password is deleted from the One Identity Manager database following publishing to the existing user accounts. The central password is not available for new user accounts.
QER Person UseCentralPassword SyncToSystemPassword	This configuration parameter defines whether the employee's central password is copied to the employee's system user password.
QER Person UseCen-	This configuration parameter specifies if the employee's

Configuration parameter	Description
tralPassword SyncToSystemPassword UnlockByCentralPassword	system user account is unlocked when the central password is synchronized.
SysConfig	If this configuration parameter is set, you can configure general settings for system behavior.
SysConfig Display	If the configuration parameter is set, user interface design is supported.
SysConfig Display SourceDetective	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.

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 75: Configuration parameter

Configuration parameter	Description
Hardware	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.
Hardware AssetAccounting	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.
Hardware Display	This configuration parameter specifies how device properties are displayed can be configured.
Hardware Display CustomHardwareType	This configuration parameter specifies whether new device with the appropriate device model is displayed on the custom form.
Hardware Display CustomHardwareType MobilePhone	This configuration parameter contain data for a device type, which represents a mobile phone.
Hardware Display CustomHardwareType Monitor	This configuration parameter contains data for a device type, which represents a monitor.
Hardware Display CustomHardwareType PC	This configuration parameter contains data for a device type, which represents a PC.

Configuration parameter	Description
Hardware Display CustomHardwareType Printer	This configuration parameter contains data for a device type, which represents a printer.
Hardware Display CustomHardwareType Server	This configuration parameter contains data for a device type, which represents a server.
Hardware Display CustomHardwareType Tablet	This configuration parameter contains data for a device type, which represents a tablet.
Hardware Display DisplayResolutions	This configuration parameter contains a pipe delimited list of all screen resolutions that are available for selection for the device's master data form.
Hardware Display MachineWithRPL	This configuration parameter specifies whether data for remote rebooting of workstations and server can be edited.
Hardware Workdesk	If this configuration parameter is set, workdesk administration is supported.
Hardware Workdesk WorkdeskAuto	This configuration parameter specifies whether a workdesk is automatically created in association with setting up a workstation or server.

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 92
- application role
 - administrators 30, 72
 - approver 36
 - approver (IT) 36
 - assign employees 116
 - attestors 30, 35
- base roles
 - employee manager 72
- employee manager 72
- Identity Management
 - employees
 - administrators 72
 - organizations
 - administrators 30
 - attestors 30
- assignment
 - about IT Shop request 18
 - company resources 23
 - direct 14
 - dynamic role 17
 - indirect 15
 - primary 16
 - configurations 16
 - secondary 15
 - configurations 25
 - permit 25

B

- base object
 - mail template 76
- business partner 74, 134

C

- company resources
 - assign 14, 52, 110, 143, 150
- configuration parameter 182, 184, 187
- cost center
 - administrators 30
 - allow assignment 25
 - approver 36, 42
 - approver (IT) 36, 42
 - assign company resources 23, 52
 - assign devices 51, 144
 - assign employees 51, 113
 - assign workdesk 152
 - assign workdesks 51
 - attestors 30, 35, 42
 - basics 10
 - conflicting roles 28, 61
 - country 44
 - dynamic 59
 - edit 42
 - functional area 44
 - IT operating data 54
 - manager 42
 - no inheritance 26, 42

- profit 44
- risk index 44
- rule violation 44
- short name 42
- state 44
- transparency index 44
- turn over 44

D

department

- administrators 30
- allow assignment 25
- approver 36, 38
- approver (IT) 36, 38
- assign company resources 23, 52
- assign devices 51, 144
- assign employees 51, 113
- assign workdesk 152
- assign workdesks 51
- attestors 30, 35, 38
- basics 10
- conflicting roles 28, 61
- contact data 40
- country 41
- dynamic 59
- edit 38
- functional area 41
- IT operating data 54
- manager 38
- no inheritance 26, 38
- object ID 38
- profit 41
- risk index 41
- rule violation 41
- short name 38

- state 41
- transparency index 41
- turn over 41

device

- assign business role 139, 145
- assign company resources 143
- assign cost center 139, 144
- assign department 139, 144, 159
- assign location 139, 144
- assign to workdesk 139, 156
- company 134
- device ID 139
- device model 131, 139
- device status 135, 159
- edit 137
- enter call 146
- location 159
- network configuration 141
- no inheritance 26, 139
- service agreement 146
- storage class 157, 159
- storage data 157
- storage type 158-159
- workdesk 147

device model

- device type 132
- disable 132
- edit 131
- local periphery 132
- logic PC 132
- PC 132
- server 132

device status 135

device type 132

devices

- assign cost center 51
- assign department 51
- assign location 51

direction of inheritance 10

dynamic role

- calculate 68-69
- calculation schedule 65
- condition 65
 - test 67
- cost center 59
- department 59
- location 59
- set up 65

E

employee

- access restriction 108
- add to IT Shop 115
- address 84
- administrators 72
- assign application role 116
- assign business role 82, 114
- assign company resources 110
- assign cost center 51, 82, 113
- assign department 51, 82, 113
- assign extended properties 123
- assign location 51, 113
- assign reports 118
- assign resource 116
- assign software 117
- assign system role 117
- assign to workdesk 80, 156
- central password 85, 89
 - password question 124

reset 125

- central SAP user account 85
- central user account 85, 88
- certification status 80, 109
- company 74, 80
- country 84, 126-127
- default email address 85, 90
- delete 96
- delete permissions 96
- deputy 82
- dummy employee 85
- employee manager 72
- enter call 123
- entry date 82
- external 80
- identity 85
- identity card number 82
- image 84
- language 84, 126
- leaving date 82
- location 84
- locked 108
- log 79
- logins 85
- main identity 85, 91
- manager 82
- managerial scope 122
- mutual aid 124-125
- new user 108
- no inheritance 26, 80
- permanently disabled 80, 94
- phone 84
- reenable 94-95
- report 128
- risk index 80

- security key (WebAuthn) 124
- security risk 80
- Starling 2FA user ID 85
- state 84, 126-127
- subidentity 91
- system user 85
- temporarily disabled 82, 94
- user account 122
- work hours 127
- X500 person 85
- employee manager 72
- extended property 176
 - assign objects 180
 - assign resource 171
 - assign to employee 123
 - create 178
 - overview form 180
 - property group 178, 181
 - scope limit 178-179

F

- functional area 34

G

- group identity 92

I

- identity
 - organizational 92
 - primary 92
- inheritance
 - abort 12
 - bottom-up 10
 - calculate 18-19, 21

- limit 26
- top-down 10
- XIsInEffect 21
- XOrigin 21
- inheritance exclusion 28
 - define for roles 61
- IT operating data 54
 - change 58

L

- leaser 74, 134
- location
 - address 48-49
 - administrators 30
 - allow assignment 25
 - approver 36, 46
 - approver (IT) 36, 46
 - assign company resources 23, 52
 - assign devices 51, 144
 - assign employees 51, 113
 - assign workdesk 152
 - assign workdesks 51
 - attestors 30, 35, 46
 - basics 10
 - conflicting roles 28, 61
 - country 48
 - dynamic 59
 - edit 46
 - functional area 50
 - IT operating data 54
 - manager 46
 - network configuration 49
 - no inheritance 26, 46
 - profit 50
 - risk index 50

- rule violation 50
- short name 46
- state 48
- transparency index 50
- turn over 50

M

- mail definition 78
- mail template
 - base object 76, 78
- manufacturer 74, 134
- mutual aid 124-125

N

- notification
 - mail template 75

O

- overview form
 - extended property 180
 - resource 171

P

- password
 - central 85, 89
 - password question 124
 - reset 125
- password policy 96
 - assign 98
 - character sets 103
 - check password 107
 - conversion script 104-105
 - default policy 98, 101

- display name 101
- edit 100
- error message 101
- excluded list 106
- failed logins 101
- generate password 107
- initial password 101
- name components 101
- password age 101
- password cycle 101
- password length 101
- password strength 101
- predefined 97
- test script 104
- property group 176
 - add 177
 - assign extended properties 181

R

- resource 163
 - assign extended properties 171
 - assign system role 170
 - assign to employee 116, 166
 - inheritance 166, 173
 - overview form 171
 - requestable 166, 173
 - resource type 166, 173
 - risk index 166, 173
 - service item 166, 173
 - set up 165
- resource type 166, 173
 - set up 165
- risk assessment
 - functional area 34

- risk index
 - for resource 166, 173
- role
 - conflicting roles 28
- role classes 33
- role type 34
- roles
 - allow assignment 25
 - assign company resources 23
 - basics 10
 - inheritance
 - bottom-up 10
 - top-down 10
 - no inheritance 26

S

- service identity 92
- service item
 - for resource 166, 173
- software
 - assign to employee 117
 - assign to workdesks 154
- sponsored identity 92
- storage class 157
- storage type 158
- subscribable report
 - assign to employee 118
- supplier 74, 134
- system role
 - add resource 170
 - assign to employee 117
 - assign to workdesk 154
- system user 85
 - locked 108

T

- template
 - IT operating data, modify 58

U

- user account
 - apply template 58

W

- workdesk
 - assign business role 148, 153
 - assign company resources 150
 - assign cost center 51, 148, 152
 - assign department 51, 149, 152
 - assign device 156
 - assign employees 156
 - assign location 51, 149, 152
 - assign software 154
 - assign system role 154
 - create automatically 147
 - edit 147
 - no inheritance 26, 148
 - status 148
 - workdesk status 136
 - workdesk type 136, 148
- workdesk status 136
- workdesk type 136