One Identity Manager 8.1.1

Identity Management Base Module Administration Guide
Copyright 2019 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 indicates a potential for property damage, personal injury, or death.

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

ℹ️ IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

One Identity Manager Identity Management Base Module Administration Guide
Updated - August 2019
Version - 8.1.1
## Contents

**Basic principles for mapping company structures in One Identity Manager**  9  
Basic principles of hierarchical role structure .................................................. 10  
Inheritance directions within a hierarchy .......................................................... 10  
Discontinuing inheritance .......................................................... 12  
Basic principles for assigning company resources .................................. 14  
Direct assignment ...................................................................................... 14  
Indirect assignment ..................................................................................... 14  
  Secondary assignment ............................................................................. 15  
  Primary assignment ................................................................................ 16  
Assignment by dynamic roles ..................................................................... 17  
Assignments via IT Shop requests ............................................................... 17  
Basic principles for calculating inheritance .............................................. 18  
Calculating inheritance by hierarchical roles ............................................. 19  
Calculation of assignments ...................................................................... 20  
Preparing hierarchical roles for company resource assignments ................ 22  
  Possible assignments of company resources through roles ...................... 22  
Permitting assignments of employees, devices, workdesks, and company resources 24  
Using roles to limit inheritance ...................................................... 26  
Inheritance exclusion: Specifying conflicting roles .................................... 27  

**Managing departments, cost centers, and locations** ................................ 29  
One Identity Manager users for organizations ............................................. 29  
Basic data for structuring departments, cost centers, and locations ............ 31  
  Role classes .......................................................................................... 32  
  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 ......................................... 45
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
  Assigning organizations ........................................................... 60
  Specifying inheritance exclusion for roles ................................ 61
  Specifying role relations ........................................................ 62
Reports about departments, cost centers, and locations .................. 63

**Working with dynamic roles** .................................................. 65
Editing dynamic roles ............................................................... 66
  Dynamic role master data ........................................................ 67
Testing a condition of a dynamic role ........................................... 68
Calculating role memberships ..................................................... 69
Additional tasks for dynamic roles .............................................. 70
  Dynamic role overview .......................................................... 70
  Start immediate recalculation of role memberships ................. 70

**Employee administration** ..................................................... 72
One Identity Manager users for employee administration .................. 73
Basic data for employee master data ............................................ 74
  Business partners ................................................................... 75
Creating custom mail templates for notifications ......................... 76
  General properties of a mail template ..................................... 77
  Creating and editing an email definition .................................. 78
Customizing email signatures ................................................................. 79
Entering employee master data .................................................................. 79
  General employee master data .............................................................. 80
  Organizational employee master data ..................................................... 83
  Address data ......................................................................................... 84
  Miscellaneous employee master data ..................................................... 86
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
Password policies for employees ............................................................... 96
  Predefined password policies ............................................................... 97
    Using a password policy ..................................................................... 98
      Changing the password policy for the password columns .................. 98
      Assigning password policies to departments, cost centers, locations and business roles .................................................. 99
  Editing password policies ................................................................. 100
    General master data for a password policy ........................................ 101
    Policy settings .................................................................................. 101
    Character classes for passwords ...................................................... 102
Custom scripts for password requirements ............................................. 103
  Script for checking a password ............................................................. 104
  Script for generating a password ......................................................... 105
Defining the excluded list for passwords ............................................... 106
Checking a password ............................................................................... 106
Testing generation of a password ............................................................ 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 .............................................................. 115
Assigning resources directly to employees ......................................................... 116
Assigning applications 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 ................................. 119
Analyzing role memberships and employee assignments ...................................... 121
Additional tasks for managing employees ............................................................ 122
  Employee overview ......................................................................................... 122
  Manually assigning user accounts to employees ................................................. 123
  Entering calls for an employee ........................................................................ 123
  Assigning extended properties ....................................................................... 123
  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
Basic principles for mapping company structures in One Identity Manager

One Identity Manager supplies employees in a company with company resources, for example, permissions or applications, 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

- Basic principles of hierarchical role structure on page 10
- Basic principles for assigning company resources on page 14
- Basic principles for calculating inheritance on page 18
- Preparing hierarchical roles for company resource assignments on page 22

Basic principles of hierarchical role structure

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. Applications assigned to the respective departments are also entered. An employee in retail is assigned all the applications that are allocated to their department and all those on the full structure path. In this case that is internet software, address administration, mail, and text editing.

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. Applications assigned to the respective project groups are also entered. An employee from the project group "Project lead" receives 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.
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 Block inheritance. The effects of this depend on the chosen direction of inheritance.

- Roles marked with Block inheritance 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 option "Block inheritance" 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 option Block inheritance is set for the department "Sales" in the top-down example, it results in sales employees being assigned address administration and employees in the retail department, address administration and internet software, but neither is assigned mail or text editing applications. Applications in the department "Overall organization" are, however, not assigned to retail and dealers.
Figure 3: Discontinuing Inheritance Top-Down

Example for Discontinuing Inheritance Bottom-Up

An employee from the project group "Programming" receives applications from the project group as well as those from the projects groups underneath. In this case, the development environment, assembler tool and the prototyping tool. If the project group "Programming" has labeled with the option Block inheritance, it no longer passes down inheritance. As a result, only the CASE tool is assigned to employees in the project group "Project lead" along with the application project management. Applications from the projects groups "Programming", "System programming" and "Interface design" 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
- Assignments via 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.
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. Specify on the role classes (department, location, cost center, business roles, application role) whether a secondary assignment of company resources to employees, device, and workdesk is possible.
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. To do this, you use input fields for roles on the employee, device and workdesk master data forms. Primary assignment inheritance can be enable through configuration parameters. Primary assignment is enabled by default for employee objects.

Figure 8: A Primary Assignment Schema

![Primary Assignment Schema Diagram]

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

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
</tbody>
</table>
### Configuration parameter | Effect when set
--- | ---
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. 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.

**Related topics**

- [Working with dynamic roles](#) on page 65

### Assignments via 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.
Basic principles for 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.

Detailed information about this topic

- Calculating inheritance by hierarchical roles on page 19
- Calculation of assignments on page 20
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 table BaseTree. The One Identity Manager data model contains the following views:

**Table 2: BaseTree table views**

<table>
<thead>
<tr>
<th>View</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Graphical representation of departments</td>
</tr>
<tr>
<td>Locality</td>
<td>Graphical representation of locations</td>
</tr>
<tr>
<td>PROFITCENTER</td>
<td>Graphical representation of cost centers</td>
</tr>
<tr>
<td>AERole</td>
<td>Application Role Mapping</td>
</tr>
</tbody>
</table>

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

Inheritance comes from the table BaseTree. The BaseTree table can map any number of hierarchical role structures using the UID_Org - UID_ParentOrg relationship. These are stored in the table BaseTreeCollection. 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 table BaseTreeCollection:

- 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 table OrgRoot ("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.
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 an application is assigned to a parent application, the members of the table BaseTreeHasApp are recalculated.

The members of a role inherit all assignments that belong to them according to the BaseTree and also previous structures according to BaseTreeCollection through primary and secondary role structures.

### 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 a column XOrigin. 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.

XIsInEffect shows whether an assignment is in effect. For example, if an employee is disabled, 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 column XIsInEffect is recalculated when changes are made to the value in XOrigin.

### Table 3: Possible values for column XOrigin

<table>
<thead>
<tr>
<th>Bit 3</th>
<th>Bit 2</th>
<th>Bit 1</th>
<th>Bit 0</th>
<th>Value in XOrigin</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>Only directly assigned.</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>Only indirectly assigned.</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>Directly and indirectly assigned.</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>Assigned through dynamic roles.</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>Assigned directly and through dynamic roles.</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>Assigned indirectly and through dynamic roles.</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>7</td>
<td>Assigned directly, indirectly and through dynamic roles.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>Assignment request</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>9</td>
<td>Assignment request and direct assignment.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>10</td>
<td>Assignment request and indirect assignment.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td>Assignment request, direct and indirect assignment.</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>Assignment request and through dynamic roles.</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>13</td>
<td>Assignment request, directly and through dynamic roles.</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>14</td>
<td>Assignment request, indirectly and through dynamic roles.</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>15</td>
<td>Assignment request, directly, indirectly and through dynamic roles.</td>
</tr>
</tbody>
</table>
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 22
- Permitting assignments of employees, devices, workdesks, and company resources on page 24
- Using roles to limit inheritance on page 26
- Inheritance exclusion: Specifying conflicting roles on page 27

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

<table>
<thead>
<tr>
<th>Assignable Company Resource</th>
<th>Members in Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>possible</td>
</tr>
<tr>
<td>Account definitions</td>
<td>possible</td>
</tr>
<tr>
<td>Groups of custom target systems</td>
<td>possible (assigns to all an employee's custom defined target systems user accounts, for which group inheritance is authorized)</td>
</tr>
<tr>
<td>Active Directory groups</td>
<td>possible (assigns to all an employee's Active Directory user accounts and Active Directory contacts, for which group inheritance is authorized)</td>
</tr>
<tr>
<td>SharePoint groups</td>
<td>possible (assigns to all an employee's SharePoint user accounts)</td>
</tr>
<tr>
<td>SharePoint roles</td>
<td>possible (assigns to all an employee's SharePoint user accounts)</td>
</tr>
<tr>
<td>LDAP groups</td>
<td>possible (assigns to all an employee's LDAP user accounts for which group inheritance is authorized)</td>
</tr>
<tr>
<td>Notes groups</td>
<td>possible (assigns to all an employee's Notes user accounts)</td>
</tr>
<tr>
<td>SAP groups</td>
<td>possible (assigns to all an employee's SAP user accounts in the same SAP client)</td>
</tr>
<tr>
<td>SAP profiles</td>
<td>possible (assigns to all an employee's SAP user accounts in the same SAP client)</td>
</tr>
<tr>
<td>SAP roles</td>
<td>possible (assigns to all an employee's SAP user accounts in the same SAP client)</td>
</tr>
<tr>
<td>Structural profiles</td>
<td>possible (assigns to all an employee's SAP user accounts in the same SAP client)</td>
</tr>
<tr>
<td>BI analysis authorizations</td>
<td>possible (assigns to all an employee's BI user accounts in the same system)</td>
</tr>
<tr>
<td>Azure Active Directory groups</td>
<td>possible (assigns to all an employee's Azure Active Directory user accounts for which group inheritance is authorized)</td>
</tr>
<tr>
<td>Assignable Company Resource</td>
<td>Members in Roles</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Azure Active Directory administrator roles</td>
<td>possible (assigns to all an employee's Azure Active Directory user accounts for which group inheritance is authorized)</td>
</tr>
<tr>
<td>Azure Active Directory subscriptions</td>
<td>possible (assigns to all an employee's Azure Active Directory user accounts for which group inheritance is authorized)</td>
</tr>
<tr>
<td>Disabled Azure Active Directory service plans</td>
<td>possible (assigns to all an employee's Azure Active Directory user accounts for which group inheritance is authorized)</td>
</tr>
<tr>
<td>Unix groups</td>
<td>possible (assigns to all an employee's Unix user accounts)</td>
</tr>
<tr>
<td>PAM user groups</td>
<td>possible (assigns to all an employee's PAM user accounts for which group inheritance is authorized)</td>
</tr>
<tr>
<td>System roles</td>
<td>possible</td>
</tr>
<tr>
<td>Subscribable reports</td>
<td>possible</td>
</tr>
<tr>
<td>Applications</td>
<td>possible</td>
</tr>
</tbody>
</table>

**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 from hierarchical roles in One Identity Manager. Role classes are used to group similar roles together. The following role classes are available by default in One Identity Manager:

- Department
- Cost center
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 Manager directly to a department, set **Assignment allowed** and **Direct assignment allowed** on "department" for "employees".

If employees can only obtain membership in a department through the IT Shop, set **Assignment allowed** but not **Direct assignment allowed** on the role class "department" for "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 task **Configure role assignments**.
3. Use the column **Allow assignments** to specify whether assignment is generally allowed.

  **NOTE:** You can only reset **Assignment allowed** 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 **Allow direct assignments** to specify whether a direct assignment is allowed.

  **NOTE:** You can only reset **Direct assignment allowed** 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 Block inheritance 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 option Block inheritance 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 Block inheritance.
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. Enable
   - Employees do not inherit
   - Devices do not inherit
     - OR -
   - Workdesks do not inherit
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 No inheritance.
   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 No inheritance.
   
   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 No inheritance.
   
   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.
To configure inheritance exclusion

- Set the configuration parameter **QER | Structures | ExcludeStructures** in the Designer 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 applications. 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: User Tasks

<table>
<thead>
<tr>
<th>User</th>
<th>Task</th>
</tr>
</thead>
</table>
| Administrators for organizations          | Administrators must be assigned to the application role **Identity Management | Organizations | Administrators**.  
Users with this application role:  
- 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       | • Create customized permissions groups for application roles for role-based login to administration tools in Designer as required.  
• Create system users and permissions groups for non-role-based login to administration tools in Designer as required.  
• Enable or disable additional configuration parameters in Designer as required.  
• Create custom processes in Designer as required.  
• Create and configure schedules as required.  
• Create and configure password policies as required.  
| Approvers for organizations               | Attestors must be assigned to the application role **Identity Management | Organizations | Attestors** or a child application role.  
Users with this application role:  
- 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.  
| NOTE:                                     | This application role is available if the module Attestation Module is installed.  
| Approvers for organizations               | Role approvers must be assigned to the **Identity Management | Organizations | Role approvers** application role or a child application role.  
Users with this application role:  
- Are approvers for the IT Shop.  

**NOTE:** This application role is available if the module Attestation Module is installed.
## User | Task
--- | ---
 |  | • Approve request from departments, cost centers, and locations for which they are responsible.

| Approvers (IT) for organizations | IT role approvers must be assigned to **Identity Management | Organizations | Role approvers (IT)** or a child application role.

Users with this application role:
- 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. You can find an overview of all configuration parameters in **Base data | General | Configuration parameters** in Designer.

- **Role classes**
  
  Role classes form the basis of mapping from 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 32
- Role types on page 34
- Functional areas on page 34
- Attestors on page 35
- Role approvers and role approvers (IT) on page 36
- Appendix: Configuration parameters for managing departments, cost centers, and locations on page 185

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

NOTE: You cannot delete the default role classes. However, you can edit their master data.
To edit role classes

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

Enter the following master data for a role class.

Table 6: Role class properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role classes</td>
<td>Role class description The role class is displayed under this name in the navigation view.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Applications role whose members are authorized to approve attestation instances for all roles in this role class.</td>
</tr>
<tr>
<td></td>
<td>To create a new application role, click . Enter the application role name and assign a parent application role.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This property is available if the Attestation Module is installed.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Inherited top-down</td>
<td>Direction of inheritance top-down.</td>
</tr>
<tr>
<td></td>
<td>Top down inheritance is defined for departments, cost centers, locations, and application roles.</td>
</tr>
<tr>
<td>Inherited bottom-up</td>
<td>Direction of inheritance bottom-up</td>
</tr>
<tr>
<td>Assignments allowed</td>
<td>Specifies whether assignments of respective object types to roles of this role class are allowed in general.</td>
</tr>
<tr>
<td>Direct assignments allowed</td>
<td>Specifies whether respective object types can be assigned directly to roles of this role class.</td>
</tr>
</tbody>
</table>

Related topics

- Attestors on page 35
- Inheritance directions within a hierarchy on page 10
- Permitting assignments of employees, devices, workdesks, and company resources on page 24
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 Organizations | Basic configuration data | Role types.
2. Select the role type in the result list. Select Change master data.
   - 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 7: Role type properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role type</td>
<td>Role type description</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

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

You want 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 category **Organizations | Basic configuration data | Functional areas**.
2. In the result list, select a function area and run the task **Change master data**.
   - 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 8: Functional area properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional area</td>
<td>Description of the functional area</td>
</tr>
<tr>
<td>Parent Functional area</td>
<td>Parent functional area in a hierarchy. Select a parent functional area from the list in order to organize your functional areas hierarchically.</td>
</tr>
<tr>
<td>Max. number of rule violations</td>
<td>List of rule violation valid for this functional area. This value can be evaluated during the rule check.</td>
</tr>
</tbody>
</table>

NOTE: This input field is available if the Compliance Rules Module exists.

| Description | Spare text box 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 9: Default application roles for attestors

<table>
<thead>
<tr>
<th>User</th>
<th>Task</th>
</tr>
</thead>
</table>
| Approvers for organizations | Attestors must be assigned to the application role **Identity Management | Organizations | Attestors** or a child application role. Users with this application role:  
  - 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.  

  ![](image.png) **NOTE:** This application role is available if the module Attestation Module is installed.

**To specify attestors**

1. Select **Organizations | Basic configuration data | Attestors**.
2. Select **Assign employees**.
3. Assign employees in **Add assignments**.

  ![](image.png) **TIP:** In the **Remove assignments** area, you can remove the assignment of employees.

  **To remove an assignment**
  - Select the employee and double-click ✓.
4. Save the changes.

**Related topics**

- **Role classes** on page 32
- 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 10: Default application roles for approvers

<table>
<thead>
<tr>
<th>User</th>
<th>Task</th>
</tr>
</thead>
</table>
| Approvers for organizations | Role approvers must be assigned to the Identity Management | Organizations | Role approvers application role or a child application role. Users with this application role:  
  - Are approvers for the IT Shop.  
  - Approve request from departments, cost centers, and locations for which they are responsible. |
| Approvers (IT) for organizations | IT role approvers must be assigned to Identity Management | Organizations | Role approvers (IT) or a child application role. Users with this application role:  
  - 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 Organizations | Basic configuration data | Approver.  
   - OR -  
   Select Organizations | Basic configuration data | Approver (IT).
2. Select Assign employees.
3. Assign employees in Add assignments.  
   - OR -  
   Remove employees from Remove assignments.
4. Save the changes.

Related topics

- One Identity Manager IT Shop Administration Guide
Editing departments

To edit departments
1. Select Organizations | Departments.
2. Select a department in the result list. Select Change master data.
   - 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 11: General Master Data for a Department

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department Name</td>
<td>Name of the department</td>
</tr>
<tr>
<td>Short name</td>
<td>Short name of the department</td>
</tr>
<tr>
<td>Object ID</td>
<td>Unique department object ID. The object ID is required, for example, in SAP systems for assigning employees to departments.</td>
</tr>
<tr>
<td>Parent department</td>
<td>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.</td>
</tr>
<tr>
<td>Role type</td>
<td>Role types for more detailed classification.</td>
</tr>
<tr>
<td>Location</td>
<td>Location to which the department is primary assigned.</td>
</tr>
<tr>
<td>Default printer server</td>
<td>Printer server for the department. Select a server from the menu to assign it to the department.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Manager</strong></td>
<td>Manager responsible for the department.</td>
</tr>
<tr>
<td>2. manager</td>
<td>Assistant manager of the department.</td>
</tr>
<tr>
<td><strong>Attestors</strong></td>
<td>Applications role whose members are authorized to approve attestation cases for this department. To create a new application role, click 🖥️. Enter the application role name and assign a parent application role.</td>
</tr>
<tr>
<td><strong>Cost center</strong></td>
<td>Cost center to which the department is primary assigned.</td>
</tr>
<tr>
<td><strong>Role approver</strong></td>
<td>Application role whose members approve IT Shop requests for members of this department. To create a new application role, click 🖥️. Enter the application role name and assign a parent application role.</td>
</tr>
<tr>
<td><strong>Role approver (IT)</strong></td>
<td>Application role whose members approve IT Shop requests for members of this department. To create a new application role, click 🖥️. Enter the application role name and assign a parent application role.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td><strong>Remarks</strong></td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td><strong>Certification status</strong></td>
<td>Certification status of the department. You can select the following certification statuses:</td>
</tr>
<tr>
<td></td>
<td>- New – The department was newly added to the One Identity Manager database.</td>
</tr>
<tr>
<td></td>
<td>- Certified – Department master data was granted approval by the manager.</td>
</tr>
<tr>
<td></td>
<td>- Denied – Department master data was denied approval by the manager.</td>
</tr>
<tr>
<td><strong>Import data source</strong></td>
<td>Target system or data source, from which the data set was imported.</td>
</tr>
<tr>
<td><strong>Full name</strong></td>
<td>Full name of the department include parent departments.</td>
</tr>
</tbody>
</table>
| **Disabled**      | Specifies whether the department is actively used. Set this option if the One Identity Manager 8.1.1 Identity Management Base Module Administration Guide Managing departments, cost centers, and locations
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>department is not used. This option does not have any effect on the calculation of inheritance.</td>
<td></td>
</tr>
<tr>
<td>Block inheritance</td>
<td>Specifies whether inheritance for this department can be discontinued. Set this option to discontinue inheritance within the department hierarchy.</td>
</tr>
<tr>
<td>X500 nodes</td>
<td>Select this option to label a department for exporting to an X500 schema.</td>
</tr>
<tr>
<td>Employees do not inherit</td>
<td>Specifies whether employee inheritance should be temporarily prevented for this department.</td>
</tr>
<tr>
<td>Devices do not inherit</td>
<td>Specifies whether device inheritance should be temporarily prevented for this department.</td>
</tr>
<tr>
<td>Workdesks do not inherit</td>
<td>Specifies whether workdesk inheritance should be temporarily prevented for this department.</td>
</tr>
<tr>
<td>Dynamic roles not allowed</td>
<td>Specifies whether a dynamic role can be created for the department.</td>
</tr>
<tr>
<td>Spare field no. ...</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
<tr>
<td>Spare date no. ...</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

**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 12: Contact data for departments

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email addresses</td>
<td>Email addresses for the department.</td>
</tr>
<tr>
<td>Visitors address</td>
<td>Department address for visitors.</td>
</tr>
<tr>
<td>Visiting hours</td>
<td>Department hours for visitors.</td>
</tr>
<tr>
<td>Phone hours</td>
<td>Department telephone hours.</td>
</tr>
<tr>
<td>Business hours</td>
<td>Department business hours.</td>
</tr>
<tr>
<td>Zip code</td>
<td>Department's zip code.</td>
</tr>
</tbody>
</table>

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 13: Master data of a department's functional area

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Country. You require this to determine the employee’s language and working hours.</td>
</tr>
<tr>
<td>State</td>
<td>State. You require this to determine the employee’s language and working hours.</td>
</tr>
<tr>
<td>Functional area</td>
<td>Department functional area This data is required for department's risk assessment.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>A risk index is calculated for the department risk assessment based on assigned company resources. The input field is only visible if the &quot;QER</td>
</tr>
<tr>
<td>Transparency index</td>
<td>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</td>
</tr>
<tr>
<td>Max. number of rule violations</td>
<td>Specify how many rule violations are permitted for this department. The value can be evaluated when compliance rules are checked.</td>
</tr>
<tr>
<td>Turnover for this unit</td>
<td>Turnover for this department.</td>
</tr>
</tbody>
</table>

NOTE: This property is only available if the Compliance Rules Module is installed.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earnings for this unit</td>
<td>Earnings for this department.</td>
</tr>
</tbody>
</table>

**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 category *Organizations | Cost centers*.  
2. Select a cost center in the result list. Select *Change master data*.  
   - 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 45  
- Setting up IT operating data on page 54

**General master data for a cost center**

Enter the following data for a cost center.

**Table 14: General Master Data for Cost Center**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost center</td>
<td>Cost center name.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Short name</td>
<td>Cost center short name.</td>
</tr>
<tr>
<td>Parent cost center</td>
<td>Parent of cost center in the hierarchy.</td>
</tr>
<tr>
<td></td>
<td>To organize cost centers hierarchically, select the parent cost center in the menu. Leave this field empty if the cost center is at the top level of the cost center hierarchy.</td>
</tr>
<tr>
<td>Role type</td>
<td>Role types for more detailed classification.</td>
</tr>
<tr>
<td>Manager</td>
<td>Manager responsible for the cost center.</td>
</tr>
<tr>
<td>Deputy manager</td>
<td>Deputy cost center manager.</td>
</tr>
<tr>
<td>Attestors</td>
<td>Applications role whose members are authorized to approve attestation cases for this cost center.</td>
</tr>
<tr>
<td></td>
<td>To create a new application role, click 🚀. Enter the application role name and assign a parent application role.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This property is available if the Attestation Module is installed.</td>
</tr>
<tr>
<td>Department</td>
<td>Department to which the cost center is primary assigned.</td>
</tr>
<tr>
<td>Location</td>
<td>Location to which the cost center is primary assigned.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Application role whose members approve IT Shop requests for members of this cost center.</td>
</tr>
<tr>
<td></td>
<td>To create a new application role, click 🚀. Enter the application role name and assign a parent application role.</td>
</tr>
<tr>
<td>Role approver (IT)</td>
<td>Application role whose members approve IT Shop requests for members of this cost center.</td>
</tr>
<tr>
<td></td>
<td>To create a new application role, click 🚀. Enter the application role name and assign a parent application role.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Comment</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Remarks</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Certification status</td>
<td>Certification status of the cost center. You can select the following certification statuses:</td>
</tr>
<tr>
<td></td>
<td>• New – The cost center was newly added to the One Identity Manager database.</td>
</tr>
<tr>
<td></td>
<td>• Certified – Cost center master data was granted approval by the manager</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Denied</td>
<td>Cost center master data was denied approval by the manager.</td>
</tr>
<tr>
<td>Import data source</td>
<td>Target system or data source, from which the data set was imported.------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disabled</td>
<td>Specifies whether the cost center is actively used. Set this option if the cost center is not used. This option does not have any effect on the calculation of inheritance.</td>
</tr>
<tr>
<td>Block inheritance</td>
<td>Specifies whether inheritance for this cost center can be discontinued. Set this option to discontinue inheritance within the cost center hierarchy.</td>
</tr>
<tr>
<td>X500 nodes</td>
<td>Select this option to label a cost center for exporting to an X500 schema.</td>
</tr>
<tr>
<td>Employees do not inherit</td>
<td>Specifies whether employee inheritance should be temporarily prevented for this cost center.</td>
</tr>
<tr>
<td>Devices do not inherit</td>
<td>Specifies whether device inheritance should be temporarily prevented for this cost center.</td>
</tr>
<tr>
<td>Workdesks do not inherit</td>
<td>Specifies whether workdesk inheritance should be temporarily prevented for this cost center.</td>
</tr>
<tr>
<td>Dynamic roles not allowed</td>
<td>Specifies whether a dynamic role can be created for the cost center.</td>
</tr>
<tr>
<td>Spare field no. 01 ... Spare field no. 10</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
<tr>
<td>Spare date no. 01 ... Spare field no. 03</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

**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 15: Master data of a cost center's functional area

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Country. You require this to determine the employee’s language and working hours.</td>
</tr>
<tr>
<td>State</td>
<td>State. You require this to determine the employee’s language and working hours.</td>
</tr>
<tr>
<td>Functional area</td>
<td>Cost center's function area. This data is required for cost center's risk assessment.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>A risk index is calculated for the cost center risk assessment based on assigned company resources. The input field is only visible if the “QER</td>
</tr>
<tr>
<td>Transparency index</td>
<td>Specifies how well you can trace cost center assignments. Use the slider to enter a value between 0 and 1.</td>
</tr>
<tr>
<td></td>
<td>0 ... no transparency</td>
</tr>
<tr>
<td></td>
<td>1 ... full transparency</td>
</tr>
<tr>
<td>Max. number of rule violations</td>
<td>Specify how many rule violations are permitted for this cost center. The value can be evaluated when compliance rules are checked.</td>
</tr>
<tr>
<td>Turnover for this unit</td>
<td>Turnover for the cost center.</td>
</tr>
<tr>
<td>Earnings for this unit</td>
<td>Earnings for the cost center.</td>
</tr>
</tbody>
</table>

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 category Organizations | Locations.
2. Select a location in the result list. Select Change master data.
   - 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 16: General master data for a location

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Name of the location.</td>
</tr>
<tr>
<td>Short name</td>
<td>Short name of the location.</td>
</tr>
<tr>
<td>Name</td>
<td>Additional name for the location.</td>
</tr>
<tr>
<td>Parent location</td>
<td>Parent of location in the hierarchy.</td>
</tr>
<tr>
<td></td>
<td>To organize locations hierarchically, select the parent location in the menu.</td>
</tr>
<tr>
<td></td>
<td>Leave this field empty if the location is at the top level of the location hierarchy.</td>
</tr>
<tr>
<td>Role type</td>
<td>Role types for more detailed classification.</td>
</tr>
<tr>
<td>Manager</td>
<td>Manager responsible for the location.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deputy manager</td>
<td>Assistant manager of the location.</td>
</tr>
</tbody>
</table>
| Attestors         | Applications role whose members are authorized to approve attestation cases for this location. To create a new application role, click ![icon]. Enter the application role name and assign a parent application role.  

**NOTE:** This property is available if the Attestation Module is installed. |
| Department        | Department to which the location is primary assigned.                      |
| Cost center       | Cost center to which the location is primary assigned.                     |
| Additional remarks| Spare text box for additional explanation.                                 |
| Role approver     | Application role whose members approve IT Shop requests for members of this location. To create a new application role, click ![icon]. Enter the application role name and assign a parent application role. |
| Role approver (IT)| Application role whose members approve IT Shop requests for members of this location. To create a new application role, click ![icon]. Enter the application role name and assign a parent application role. |
| Description       | Spare text box for additional explanation.                                 |
| Comment           | Spare text box for additional explanation.                                 |
| Remarks           | Spare text box for additional explanation.                                 |
| Certification status | Certification status of the location. You can select the following certification statuses:  

- 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. |
<p>| Import data source| Target system or data source, from which the data set was imported.        |
| Disabled          | 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. |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block inheritance</td>
<td>Specifies whether inheritance for this location can be discontinued. Set this option to discontinue inheritance within the location hierarchy.</td>
</tr>
<tr>
<td>X500 nodes</td>
<td>Select this option to label a location for exporting to an X500 schema.</td>
</tr>
<tr>
<td>Employees do not inherit</td>
<td>Specifies whether employee inheritance should be temporarily prevented for this location.</td>
</tr>
<tr>
<td>Devices do not inherit</td>
<td>Specifies whether device inheritance should be temporarily prevented for this location.</td>
</tr>
<tr>
<td>Workdesks do not inherit</td>
<td>Specifies whether workdesk inheritance should be temporarily prevented for this location.</td>
</tr>
<tr>
<td>Dynamic roles not allowed</td>
<td>Specifies whether a dynamic role can be created for the location.</td>
</tr>
<tr>
<td>Spare field no. 01 ... Spare field no. 10</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
<tr>
<td>Spare date no. 01 ... Spare field no. 03</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

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 17: Location's address data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Postal address of the location.</td>
</tr>
<tr>
<td>Street</td>
<td>Street or road.</td>
</tr>
<tr>
<td>Building</td>
<td>Building</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Zip code</td>
<td>Zip code.</td>
</tr>
<tr>
<td>City</td>
<td>City.</td>
</tr>
<tr>
<td>Country</td>
<td>Country. You require this to determine the employee’s language and working hours.</td>
</tr>
<tr>
<td>State</td>
<td>State. You require this to determine the employee’s language and working hours.</td>
</tr>
<tr>
<td>Phone</td>
<td>Telephone number of the location.</td>
</tr>
<tr>
<td>Quick dial</td>
<td>Telephone short entry (without code).</td>
</tr>
<tr>
<td>Fax</td>
<td>Fax number of the location.</td>
</tr>
<tr>
<td>Room</td>
<td>Room.</td>
</tr>
<tr>
<td>Comment</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

**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 18: Location network data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP offset</td>
<td>IP offset of the location.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Subnet mask of the location.</td>
</tr>
</tbody>
</table>

**Directions to location**

Enter another address and a description of the way to reach the location. Select the button next to the input field to activate it and add add data. Use the button to remove data from the list.
Table 19: Directions to Location

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visitors address</td>
<td>Location address for visitors.</td>
</tr>
<tr>
<td>Travel directions</td>
<td>Travel directions to the location.</td>
</tr>
</tbody>
</table>

**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 20: Master data of a location's functional area

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional area</td>
<td>Location's function area. This data is required for location's risk assessment.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>A risk index is calculated for the location risk assessment based on assigned company resources. The input field is only visible if the &quot;QER</td>
</tr>
</tbody>
</table>
| 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 Organizations | <Role class>.
2. Select the role in the result list.
3. Select the appropriate task.
   - Assign employees
   - Assign devices
   - Assign workdesk
4. Assign objects in Add assignments.
   - OR -
   Remove objects in Remove assignments.
5. Save the changes.

<i>TIP:</i> 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 21: Possible Assignments of Company Resources to Roles

<table>
<thead>
<tr>
<th>Company Resource</th>
<th>Available in Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>always</td>
</tr>
<tr>
<td>Account definitions</td>
<td>Target System Base Module</td>
</tr>
<tr>
<td>Groups of custom target systems</td>
<td>Target System Base Module</td>
</tr>
<tr>
<td>Active Directory groups</td>
<td>Active Directory Module</td>
</tr>
<tr>
<td>SharePoint groups</td>
<td>SharePoint Module</td>
</tr>
<tr>
<td>Company Resource</td>
<td>Available in Module</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>SharePoint roles</td>
<td>SharePoint Module</td>
</tr>
<tr>
<td>LDAP groups</td>
<td>LDAP Module</td>
</tr>
<tr>
<td>Notes groups</td>
<td>IBM Notes Module</td>
</tr>
<tr>
<td>SAP groups</td>
<td>SAP R/3 User Management Module</td>
</tr>
<tr>
<td>SAP profiles</td>
<td>SAP R/3 User Management Module</td>
</tr>
<tr>
<td>SAP roles</td>
<td>SAP R/3 User Management Module</td>
</tr>
<tr>
<td>Structural profiles</td>
<td>SAP R/3 Structural Profiles Add-on Module</td>
</tr>
<tr>
<td>BI analysis authorizations</td>
<td>SAP R/3 Analysis Authorizations Add-on Module</td>
</tr>
<tr>
<td>E-Business Suite permissions</td>
<td>Oracle E-Business Suite Module</td>
</tr>
<tr>
<td>System roles</td>
<td>System Roles Module</td>
</tr>
<tr>
<td>Subscribable reports</td>
<td>Report Subscription Module</td>
</tr>
<tr>
<td>Applications</td>
<td>Application Management Module</td>
</tr>
<tr>
<td>Azure Active Directory groups</td>
<td>Azure Active Directory Module</td>
</tr>
<tr>
<td>Azure Active Directory administrator roles</td>
<td>Azure Active Directory Module</td>
</tr>
<tr>
<td>Azure Active Directory subscriptions</td>
<td>Azure Active Directory Module</td>
</tr>
<tr>
<td>Disabled Azure Active Directory service plans</td>
<td>Azure Active Directory Module</td>
</tr>
<tr>
<td>Unix groups</td>
<td>Unix Based Target Systems Module</td>
</tr>
<tr>
<td>Cloud groups</td>
<td>Cloud Systems Management Module</td>
</tr>
<tr>
<td>PAM user groups</td>
<td>Privileged Account Governance Module</td>
</tr>
<tr>
<td>G Suite groups</td>
<td>G Suite Module</td>
</tr>
<tr>
<td>G Suite products and SKUs</td>
<td>G Suite Module</td>
</tr>
</tbody>
</table>

**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. Assign company resources in **Add assignments**.
   - OR -
   In the **Remove assignments** area, 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 24

Related topics

- Possible assignments of company resources through roles on page 22
- Assigning employees, devices and workdesks to departments, cost centers, and locations on page 51
- Working with dynamic roles on page 65

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 domainA. In addition, certain employees in department A obtain administrative user accounts in the domainA.

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 property "Department" 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, specify the effective account definition B IT operating data for department A. This IT operating data is used for administrative user accounts.
To define IT operating data

1. In 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 22: IT operating data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effects on</td>
<td>IT operating data application scope. The IT operating data can be used for a target system or a defined account definition.</td>
</tr>
<tr>
<td></td>
<td>To specify an application scope</td>
</tr>
<tr>
<td></td>
<td>a. Click ➔ next to the text box.</td>
</tr>
<tr>
<td></td>
<td>b. Under Table, select the table that maps the target system for select the TSBAccountDef table for an account definition.</td>
</tr>
<tr>
<td></td>
<td>c. Select the specific target system or account definition under Effects on.</td>
</tr>
<tr>
<td></td>
<td>d. Click OK.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Column</th>
<th>User account property for which the value is set.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the One Identity Manager Target System Base Module Administration Guide.</td>
</tr>
<tr>
<td>Value</td>
<td>Concrete value which is assigned to the user account property.</td>
</tr>
</tbody>
</table>

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 23: Target system dependent IT operating data

<table>
<thead>
<tr>
<th>Target system type</th>
<th>IT operating data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Container</td>
</tr>
<tr>
<td></td>
<td>Home server</td>
</tr>
<tr>
<td></td>
<td>Profile server</td>
</tr>
<tr>
<td></td>
<td>Terminal home server</td>
</tr>
<tr>
<td></td>
<td>Terminal profile server</td>
</tr>
<tr>
<td></td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td>Microsoft Exchange</td>
<td>Mailbox database</td>
</tr>
<tr>
<td>LDAP</td>
<td>Container</td>
</tr>
<tr>
<td></td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td>IBM Notes</td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>Certificate</td>
</tr>
<tr>
<td></td>
<td>Template for mail file</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Authentication mode</td>
</tr>
<tr>
<td></td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td>SharePoint Online</td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td></td>
<td>Authentication mode</td>
</tr>
<tr>
<td>Custom target systems</td>
<td>Container (per target system)</td>
</tr>
<tr>
<td></td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td>Target system type</td>
<td>IT operating data</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Azure Active Directory</td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td></td>
<td>Change password at next login</td>
</tr>
<tr>
<td>Cloud target system</td>
<td>Container (per target system)</td>
</tr>
<tr>
<td></td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td>Unix-based target system</td>
<td>Login shell</td>
</tr>
<tr>
<td></td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td>Oracle E-Business Suite</td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td>Exchange Online</td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td>Privileged Account Management</td>
<td>Authentication provider</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td>G Suite</td>
<td>Organization</td>
</tr>
<tr>
<td></td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Groups can be inherited</td>
</tr>
<tr>
<td></td>
<td>Privileged user account</td>
</tr>
<tr>
<td></td>
<td>Change password at next login</td>
</tr>
</tbody>
</table>

**Related topics**

- One Identity Manager Target System Base Module Administration Guide
Modify IT operating data

If IT operating data changes, you must transfer these 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, cost center, business role, or a location was changed.
- 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 Manager, select the category <target system type> | Basic configuration data | Account definitions | Account definitions.
2. Select an account definition in the result list.
3. Select Execute templates in the task view
   This displays a list of all user account, which are created through the selected account definition and whose properties are 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 the modification shall be adopted for 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 Organizations | <Role class>.
2. Select the role in the result list.
3. Select Create dynamic role in the task view.
4. Enter the required master data.
5. Save the changes.

To edit a dynamic role

1. Select Organizations | <Role class> | Dynamic roles.
2. Select the role in the result list.
3. Open the role's overview form.
4. Select the form element Dynamic roles and click on the dynamic role.
5. Select Change master data.
6. Edit the dynamic role's master data.
7. Save the changes.

Related topics

- Working with dynamic roles on page 65
- Editing dynamic roles on page 66
- General master data for a department on page 38
Assigning organizations

Use this task to map the relationships of a department, cost center of 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 Organizations | Cost centers or Organizations | Locations.
2. Select the role in the result list.
3. Select Assign organizations.
4. Select Departments.
5. Assign departments in Add assignments.
   The selected role is assigned to all departments as cost center or location.
   - OR -
   In Remove assignments, remove the departments.
6. Save the changes.

To assign a department or a location to cost centers

1. Select Organizations | Departments or Organizations | Locations.
2. Select the role in the result list.
3. Select Assign organizations.
4. Select Cost centers.
5. Assign cost centers in Add assignments.
   The selected role is assigned to all cost centers as department or location.
   - OR -
   In Remove assignments, remove the cost centers.
6. Save the changes.

To assign a department or a cost center to locations

1. Select Organizations | Departments or Organizations | Cost centers.
2. Select the role in the result list.
3. Select Assign organizations.
4. Select Locations.
5. Assign locations in **Add assignments**.
   The selected role is assigned to all locations as department or cost center.
   - OR -
   In **Remove assignments**, 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**

- Set the configuration parameter **QER | Structures | ExcludeStructures** in the Designer and compile the database.

**To define inheritance exclusion for a departments**

1. Select **Organizations | Departments** in Manager.
2. Select the department in the result list.
3. Select **Edit conflicting departments**.
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 Manager.
2. Select the cost center in the result list.
3. Select **Edit conflicting cost centers**.
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 Manager.
2. Select the location in the result list.
3. Select **Edit conflicting locations**.
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 27

**Specifying role relations**

**Table 24: Configuration parameter for editing role relations**

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>RelatedStructures</td>
<td></td>
</tr>
</tbody>
</table>

Use this task to specify between which roles relations exist. This mapping is only for informative use. Parent node definitions do not provide information about role relations of subordinate roles.

**To define relations between departments**

1. Select **Organizations | Departments**.
2. Select the department in the result list.
3. Select **Specify department relations**.
4. Assign the departments for which relations exist in **Add assignments**.
5. Save the changes.
To define relations between cost centers
1. Select the category Organizations | Cost centers.
2. Select the cost center in the result list.
3. Select Specify cost center relations.
4. Assign the cost centers for which relations exist in Add assignments.
5. Save the changes.

To define relations between locations
1. Select the category Organizations | Locations.
2. Select the location in the result list.
3. Select Specify location relations.
4. Assign the locations for which relations exist in Add assignments.
5. Save the changes.

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 25: Reports about Departments, Cost Centers and Locations

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of all assignments</td>
<td>This report finds all the roles in which employees from the selected department, cost center, or location are also members.</td>
</tr>
<tr>
<td>Data quality of department members</td>
<td>This report evaluates the data quality of employee data records. It takes all employees in the department or cost center into account.</td>
</tr>
<tr>
<td>data center members (cost center members)</td>
<td></td>
</tr>
<tr>
<td>Show historical memberships</td>
<td>This report lists all members of the selected department, cost center, or location and the duration of their membership.</td>
</tr>
<tr>
<td>Employees per department</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Report Description

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees per cost center</td>
<td>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 <em>My One Identity Manager</em>.</td>
</tr>
<tr>
<td>Employees per location</td>
<td>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 <em>My One Identity Manager</em>.</td>
</tr>
</tbody>
</table>

### Related topics

- [Analyzing role memberships and employee assignments](#) on page 121
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. 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.

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:

<table>
<thead>
<tr>
<th>Dynamic role</th>
<th>External employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>All external employees</td>
</tr>
<tr>
<td>Object class</td>
<td>PERSON</td>
</tr>
<tr>
<td>Condition</td>
<td>IsExternal = 1</td>
</tr>
<tr>
<td>Department</td>
<td>A_1</td>
</tr>
</tbody>
</table>

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 66
- Calculating role memberships on page 69

Related topics

- Basic principles for assigning company resources on page 14
- Permitting assignments of employees, devices, workdesks, and company resources on page 24
- Appendix: Configuration parameters for managing departments, cost centers, and locations on page 185

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 Create dynamic role in the task view.
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 form element "dynamic roles" and click on the dynamic role.
4. Select Change master data.
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 26: Dynamic Role Master Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>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.</td>
</tr>
<tr>
<td>Object class</td>
<td>Object class that the dynamic role applies to. Choose between Person, Hardware and Workdesk.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Dynamic role</td>
<td>Name of the dynamic role.</td>
</tr>
<tr>
<td>Calculation schedule</td>
<td>Schedule, which triggers cyclical recalculation of the role membership. In the standard installation of the One Identity Manager, the schedule Dynamic roles check is already defined. All dynamic role memberships are checked using this schedule and if necessary, recalculation requests are sent to the DBQueue Processor. 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.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Condition</td>
<td>Defines which objects of the object class become members of the selected role. The condition is defined as a valid WHERE clause for a database query and must relate to the selected object class. You can enter the conditions directly as an SQL query or user the WHERE clause wizard. Alternatively, you can enter conditions for employee objects with the filter designer.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
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 66
- Testing a condition of a dynamic role on page 68
- Start immediate recalculation of role memberships on page 70

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 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 Change master data.
5. Click (Edit SQL) on the form.
   This displays the condition as SQL query.
6. Select Test condition in the task view.
   On the master data form, in the Test result field, all objects determined by the condition are displayed.
Calculating role memberships

Table 27: Configuration parameters for calculating dynamic roles

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
</tbody>
</table>

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 Designer, set the configuration parameters QER | Structures | DynamicGroupCheck | CalculateImmediatelyPerson, QER | Structures | DynamicGroupCheck | CalculateImmediatelyHardware and QER | Structures | DynamicGroupCheck | CalculateImmediatelyWorkdesk.

Related topics
- Start immediate recalculation of role memberships on page 70

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 Dynamic role overview in the task view.

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 Start recalculation immediately 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 69
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 the 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 configuration parameter QER | Person is set.

- Check whether the configuration parameter is set in the Designer. 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 119
- Analyzing role memberships and employee assignments on page 121
- 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 28: Users

<table>
<thead>
<tr>
<th>Users</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee administrators</td>
<td>Employee administrators must be assigned to the application role</td>
</tr>
<tr>
<td></td>
<td>**Identity Management</td>
</tr>
<tr>
<td></td>
<td>Users with this application role:</td>
</tr>
<tr>
<td></td>
<td>• Can edit master data for all employees</td>
</tr>
<tr>
<td></td>
<td>• Can assign a manager.</td>
</tr>
<tr>
<td></td>
<td>• Can assign company resources to employees.</td>
</tr>
<tr>
<td></td>
<td>• Check and authorize employee master data.</td>
</tr>
<tr>
<td></td>
<td>• Create and edit risk index functions.</td>
</tr>
<tr>
<td></td>
<td>• Edit password policies for employee passwords</td>
</tr>
<tr>
<td></td>
<td>• Delete employee's security keys (Webauthn)</td>
</tr>
<tr>
<td>Employee managers</td>
<td>**Base roles</td>
</tr>
<tr>
<td></td>
<td>Users with this application role:</td>
</tr>
<tr>
<td></td>
<td>• Can edit master data for the objects they are responsible for and assign company resources to them.</td>
</tr>
<tr>
<td></td>
<td>• Can edit master data for their employees in the Web Portal.</td>
</tr>
<tr>
<td></td>
<td>• Can add their staff members to the IT Shop.</td>
</tr>
<tr>
<td></td>
<td>• Employee and department managers can add new employees in the Web Portal.</td>
</tr>
<tr>
<td></td>
<td>• Can view their staff’s compliance rule violations in the Web Portal.</td>
</tr>
<tr>
<td></td>
<td>Members of this application role are determined through a dynamic role.</td>
</tr>
<tr>
<td>One Identity Manager</td>
<td>• Create customized permissions groups for application roles for role-based login to administration tools in Designer as required.</td>
</tr>
<tr>
<td>administrators</td>
<td>• Create system users and permissions groups for non-role-based login to administration tools in Designer as required.</td>
</tr>
<tr>
<td></td>
<td>• Enable or disable additional configuration parameters in Designer as required.</td>
</tr>
<tr>
<td></td>
<td>• Create custom processes in Designer as required.</td>
</tr>
<tr>
<td>Users</td>
<td>Task</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td>• Create and configures schedules as required.</td>
</tr>
<tr>
<td></td>
<td>• Create and configure password policies as required.</td>
</tr>
</tbody>
</table>

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

  Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. You can find an overview of all configuration parameters in **Base data | General | Configuration parameters** in Designer.

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

## Detailed information about this topic

- **Business partners** on page 75
- **Creating custom mail templates for notifications** on page 76
- **Password policies for employees** on page 96
- **Appendix: Configuration parameters for managing employees** on page 187
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. Select Employees | Basic configuration data | Business partners.
2. Select a company in the result list. Select Change master data.
   - 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 29: General master data for a company

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company</td>
<td>Short description of the company for the views in One Identity Manager tools.</td>
</tr>
<tr>
<td>Name</td>
<td>Full company name.</td>
</tr>
<tr>
<td>Surname prefix</td>
<td>Additional company name.</td>
</tr>
<tr>
<td>Short name</td>
<td>Company's short name.</td>
</tr>
<tr>
<td>Contact</td>
<td>Contact person for the company.</td>
</tr>
<tr>
<td>Partner</td>
<td>Specifies whether this is a partner company.</td>
</tr>
<tr>
<td>Customer number</td>
<td>Customer number at the partner company.</td>
</tr>
<tr>
<td>Supplier</td>
<td>Specifies whether this is a supplier.</td>
</tr>
<tr>
<td>Customer number</td>
<td>Customers number at supplier.</td>
</tr>
<tr>
<td>Leasing partner</td>
<td>Specifies whether this is a leasing provider or rental firm.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Specifies whether this is a manufacturer.</td>
</tr>
<tr>
<td>Remarks</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>
Table 30: Company address

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Street</td>
<td>Street or road.</td>
</tr>
<tr>
<td>Building</td>
<td>Building</td>
</tr>
<tr>
<td>Zip code</td>
<td>Zip code.</td>
</tr>
<tr>
<td>City</td>
<td>City.</td>
</tr>
<tr>
<td>State</td>
<td>State.</td>
</tr>
<tr>
<td>Country</td>
<td>Country.</td>
</tr>
<tr>
<td>Phone</td>
<td>Company's telephone number.</td>
</tr>
<tr>
<td>Fax</td>
<td>Company's fax number.</td>
</tr>
<tr>
<td>Email address</td>
<td>Company's email address.</td>
</tr>
<tr>
<td>Website</td>
<td>Company's website.</td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Browse</strong> button to display the web page in the default web browser.</td>
</tr>
</tbody>
</table>

Creating custom mail templates for notifications

**To edit mail templates**

1. In Manager, select the category **Employees | Basic configuration data | Mail templates**.
2. Select a mail template in the result list and run **Change master data**.
   - OR -
   Click in the result list.
   This opens the mail template editor.
3. Edit the mail template.
4. Save the changes.

**Detailed information about this topic**

- Creating and editing an email definition on page 78
- Customizing email signatures on page 79
## General properties of a mail template

The following general properties are displayed for a mail template:

### Table 31: Mail template properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail template Name</td>
<td>Name of the mail template. This name will be used to display the mail</td>
</tr>
<tr>
<td></td>
<td>templates in the administration tools and in Web Portal. Translate the</td>
</tr>
<tr>
<td></td>
<td>given text using the button.</td>
</tr>
<tr>
<td>Base object</td>
<td>Mail template base object. A base object only needs to be entered if</td>
</tr>
<tr>
<td></td>
<td>the mail definition properties of the base object are referenced.</td>
</tr>
<tr>
<td>Report (parameter set)</td>
<td>Report, made available through the mail template.</td>
</tr>
<tr>
<td>Description</td>
<td>Mail template description. Translate the given text using the button.</td>
</tr>
<tr>
<td>Target format</td>
<td>Format in which to generate email notification. Permitted values are:</td>
</tr>
<tr>
<td></td>
<td>- HTML: The email notification is formatted in HTML. Text formats,</td>
</tr>
<tr>
<td></td>
<td>for example, different fonts, colored fonts or other text</td>
</tr>
<tr>
<td></td>
<td>formatting can be included in HTML format.</td>
</tr>
<tr>
<td></td>
<td>- TXT: The email notification is formatted as text. Text format</td>
</tr>
<tr>
<td></td>
<td>does not support bold, italics or colored font or other text</td>
</tr>
<tr>
<td></td>
<td>formatting. Images displayed directly in the message are not</td>
</tr>
<tr>
<td></td>
<td>supported.</td>
</tr>
<tr>
<td>Design type</td>
<td>Design in which to generate the email notification. Permitted values</td>
</tr>
<tr>
<td></td>
<td>are:</td>
</tr>
<tr>
<td></td>
<td>- Mail template: The generated email notification contains the mail</td>
</tr>
<tr>
<td></td>
<td>body in accordance with the mail definition.</td>
</tr>
<tr>
<td></td>
<td>- Report: The generated email notification contains the report</td>
</tr>
<tr>
<td></td>
<td>specified under Report (parameter set) as its mail body.</td>
</tr>
<tr>
<td></td>
<td>- Mail template, report in attachment: The generated email</td>
</tr>
<tr>
<td></td>
<td>notification contains the mail body in accordance with the mail</td>
</tr>
<tr>
<td></td>
<td>definition. The report specified under Report (parameter set) is</td>
</tr>
<tr>
<td></td>
<td>attached to the notification as a PDF file.</td>
</tr>
<tr>
<td>Importance</td>
<td>Importance for the email notification. Permitted values are Low,</td>
</tr>
<tr>
<td></td>
<td>Normal, and High.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Confidentiality for the email notification. Permitted values are</td>
</tr>
<tr>
<td></td>
<td>Normal, Personal, Private, and Confidential.</td>
</tr>
<tr>
<td>Can unsubscribe</td>
<td>Specifies whether the recipient can unsubscribe email notification.</td>
</tr>
<tr>
<td></td>
<td>If this option is set, the emails can be unsubscribed through the</td>
</tr>
<tr>
<td></td>
<td>Web Portal.</td>
</tr>
<tr>
<td>Deactivated</td>
<td>Specifies whether this mail template is disabled.</td>
</tr>
<tr>
<td>Property</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mail definition</td>
<td>Unique name for the mail definition.</td>
</tr>
<tr>
<td>Language</td>
<td>Language which applies to the mail template. The recipient's language preferences are taken into account when an email notification is generated.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject of the email message</td>
</tr>
<tr>
<td>Mail body</td>
<td>Content of the email message</td>
</tr>
</tbody>
</table>

**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 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 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 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 32: Configuration parameters for email signatures

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
<tr>
<td>Common</td>
<td>MailNotification</td>
</tr>
</tbody>
</table>

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 term **Employee** is used in the following description.

Enter employee master data in the One Identity Manager in **Employees**. 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. Select the Employees | Employees.
2. Select an employee in the result list and run Change master data.
   – 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 83
- Address data on page 84
- Miscellaneous employee master master data on page 86

General employee master data

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

Table 33: General Master Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>Employee's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>Employee's last name.</td>
</tr>
<tr>
<td>Middle name</td>
<td>Second middle name.</td>
</tr>
<tr>
<td>Form of address</td>
<td>Employee's form of address. This is automatically set depending on gender.</td>
</tr>
<tr>
<td>Title</td>
<td>Employee's title.</td>
</tr>
<tr>
<td>Surname</td>
<td>Employee's surname prefix, for example du, or von.</td>
</tr>
<tr>
<td><strong>Property</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>prefix</td>
<td>Employee's preferred name.</td>
</tr>
<tr>
<td>Preferred name</td>
<td>Employee's preferred name. These are automatically taken from first and last names.</td>
</tr>
<tr>
<td>Initials</td>
<td>Employee's initials. These are automatically taken from first and last names.</td>
</tr>
<tr>
<td>Gender</td>
<td>Employee's gender.</td>
</tr>
<tr>
<td>Date of birth</td>
<td>Employee's date of birth.</td>
</tr>
<tr>
<td>Name at birth</td>
<td>Employee's name at date.</td>
</tr>
<tr>
<td>Job description</td>
<td>Description of employee's job within your company.</td>
</tr>
<tr>
<td>Generational affix</td>
<td>Affix, for example <strong>Senior</strong> or <strong>Junior</strong>.</td>
</tr>
<tr>
<td>Language</td>
<td>Language used for sending email notifications to the employee.</td>
</tr>
<tr>
<td>Sub-organization</td>
<td>Note about sub-organizations to which the Employee belongs.</td>
</tr>
<tr>
<td>Permanently disabled</td>
<td>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.</td>
</tr>
<tr>
<td>Certification status</td>
<td>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:</td>
</tr>
</tbody>
</table>

- **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.

<table>
<thead>
<tr>
<th>VIP</th>
<th>Labels the employee as important.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security risk</td>
<td>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.</td>
</tr>
<tr>
<td>No inheritance</td>
<td>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.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Direct assignments</td>
<td>Direct assignments remain intact.</td>
</tr>
<tr>
<td></td>
<td>If the configuration parameter **QER</td>
</tr>
<tr>
<td>External</td>
<td>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 the One Identity Manager.</td>
</tr>
<tr>
<td>Employee type</td>
<td>Type of relationship to the company Permitted values are <strong>Employee</strong>, <strong>Apprentice</strong>, <strong>Contractor</strong>, <strong>Consultant</strong>, <strong>Partner</strong>, <strong>Customer</strong>, <strong>Other</strong>.</td>
</tr>
<tr>
<td>Contact email</td>
<td>E-mail address to which the registration link is sent when a new user account is created using the Self-Registration Web Portal.</td>
</tr>
<tr>
<td>Company</td>
<td>Enter a company. Use the <img src="image" alt="add company" /> next to the text box to add a new company.</td>
</tr>
<tr>
<td>Workdesk</td>
<td>Employee's workdesk.</td>
</tr>
<tr>
<td>Risk index (calculated)</td>
<td>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 input field is only visible if the configuration parameter **QER</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Comment</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Spare field no. 01</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
<tr>
<td>Spare field no. 10</td>
<td></td>
</tr>
</tbody>
</table>

**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 75
- How to set up workdesks on page 147
## Organizational employee master data

Enter the following general master data for an organization.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel number</td>
<td>Employee's personnel number.</td>
</tr>
<tr>
<td>Primary department</td>
<td>Department to which the employee is primary assigned. The employee can obtain company resources through this assignment when One Identity Manager is configured respectively. Furthermore, IT operating data for user accounts and mailboxes can be determined though the department.</td>
</tr>
<tr>
<td>Primary cost center</td>
<td>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. Furthermore, IT operating data for user accounts and mailboxes can be determined though the cost center.</td>
</tr>
<tr>
<td>Primary business roles</td>
<td>Business role to which the employee is assigned. The employee can obtain company resources through this assignment when One Identity Manager is configured respectively. Furthermore, IT operating data for user accounts and mailboxes can be determined though the business role. <strong>NOTE:</strong> This property is available if the Business Roles Module is installed.</td>
</tr>
<tr>
<td>Security identification</td>
<td>Security code for the employee for, for example, access permission.</td>
</tr>
<tr>
<td>User account creation date</td>
<td>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.</td>
</tr>
<tr>
<td>Entry date</td>
<td>Date the employee started at the company. This is filled with the current date when the employee is added.</td>
</tr>
<tr>
<td>End date</td>
<td>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 <strong>Lock accounts of employees that have left the company.</strong> When the end date arrives, the employee is blocked.</td>
</tr>
<tr>
<td>Company member</td>
<td>Additional information about the employee’s affiliation.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporarily disabled</td>
<td>Specifies whether the employee is temporarily absent from the company If this option is set, enter the time period for the temporary absence.</td>
</tr>
<tr>
<td>Temporarily disabled from</td>
<td>Date from which the employee and associated user accounts are disabled.</td>
</tr>
<tr>
<td>Temporarily disabled until</td>
<td>Date until which the employee and associated user accounts are disabled. A schedule is implemented <strong>Enable temporarily disabled accounts</strong> that monitors the end date of the temporary deactivation. When this date is reached the employee and their user accounts are re-enabled.</td>
</tr>
<tr>
<td>Last working day</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

### Manager

An employee’s manager can assume several tasks in One Identity Manager such as

- 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 35: Address data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary location</td>
<td>Location to which the employee is primarily assigned. The employee can obtain company resources through this assignment when One Identity Manager is configured respectively. Furthermore, IT operating data for user accounts and mailboxes can be determined through the location.</td>
</tr>
<tr>
<td>Phone</td>
<td>Employee's telephone number.</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>Employee's mobile number.</td>
</tr>
<tr>
<td>Fax</td>
<td>Employee's fax number.</td>
</tr>
<tr>
<td>Display in phone book</td>
<td>Specifies whether the employee can be shown in the telephone book.</td>
</tr>
<tr>
<td>Street</td>
<td>Street or road.</td>
</tr>
<tr>
<td>Building</td>
<td>Building</td>
</tr>
<tr>
<td>Office mailbox</td>
<td>Office mailbox.</td>
</tr>
<tr>
<td>Zip code</td>
<td>Zip code.</td>
</tr>
<tr>
<td>City</td>
<td>City.</td>
</tr>
<tr>
<td>Country</td>
<td>Country. You require this to determine the employee’s language and working hours. This data is usually stored with the employee’s location or department data. You can also enter it directly by the employee.</td>
</tr>
<tr>
<td>State</td>
<td>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.</td>
</tr>
<tr>
<td>Floor</td>
<td>Floor.</td>
</tr>
<tr>
<td>Room</td>
<td>Room.</td>
</tr>
<tr>
<td>Picture</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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 36: Miscellaneous Master Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central user account</td>
<td>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.</td>
</tr>
<tr>
<td>Central SAP user account</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This property is only available if the SAP R/3 User Management Module is installed.</td>
</tr>
<tr>
<td>E-Business Suite user account</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This property is only available if the Oracle E-Business Suite Module is installed.</td>
</tr>
<tr>
<td>E-Business Suite ID</td>
<td>Unique ID for the HR employee, the AP customer, the AP supplier or the AR parties in the Oracle E-Business Suite.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This property is only available if the Oracle E-Business Suite Module is installed.</td>
</tr>
<tr>
<td>E-Business Suite employee ID</td>
<td>Personnel number of the HR employee in the Oracle E-Business Suite.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This property is only available if the Oracle E-Business Suite Module is installed.</td>
</tr>
<tr>
<td>Central password and password confirmation</td>
<td>Password for logging in to the target system. An employee's central password is formed from the target system specific user accounts by respective configuration.</td>
</tr>
<tr>
<td>Default email address</td>
<td>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</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>central user account</td>
<td>The central user account and the default mail domain of the active target system. When central user accounts are assigned, you can configure them the same way as regular user accounts.</td>
</tr>
<tr>
<td>Identity</td>
<td>Identity type of the person.</td>
</tr>
<tr>
<td>Main identity</td>
<td>Allocate a main identity here if the employee is managed as a sub-identity in the One Identity Manager. A subidentity allows you to set up special cases in One Identity Manager. If an employee has several user accounts in one target system that must be assigned to different groups, create a separate subidentity for each user account with a link to the main identity.</td>
</tr>
<tr>
<td>Dummy employee</td>
<td>Specifies whether the employee represents an actual employee or a dummy employee, which is used, for example, for connecting to administrative user accounts.</td>
</tr>
<tr>
<td>Actual employee</td>
<td>Unique ID of the actual employee.</td>
</tr>
<tr>
<td>X500 dummy</td>
<td>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 &quot;Dummy&quot; employee. Label the employee with the option <strong>X500 dummy</strong> in this case and configure a link to the real X500 employee.</td>
</tr>
<tr>
<td>X500 person</td>
<td>Assign the X500 dummy employee to an existing employee.</td>
</tr>
<tr>
<td>Logins</td>
<td>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 <strong>User account</strong> and <strong>User account (role-based)</strong> are used for logging in to One Identity Manager tools. For detailed information about the One Identity Manager authentication modules, see the <strong>One Identity Manager Authorization and Authentication Guide</strong>.</td>
</tr>
<tr>
<td>Starling 2FA user ID</td>
<td>User ID for multi-factor authentication. For detailed information about multi-factor authentication, see the <strong>One Identity Manager IT Shop Administration Guide</strong>.</td>
</tr>
<tr>
<td>System user</td>
<td>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. For detailed information about the One Identity Manager authentication modules, see the <strong>One Identity Manager Authorization and Authentication Guide</strong>.</td>
</tr>
<tr>
<td>System user password</td>
<td>Employee’s system user password. Password with which the employee logs in to the One Identity Manager tools.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>password confirmation</td>
<td>If an employee is permitted access to the mainframe with their user account, enter the login name here.</td>
</tr>
<tr>
<td>User account name (mainframe)</td>
<td>Just for information.</td>
</tr>
<tr>
<td>Notebook user</td>
<td>Just for information.</td>
</tr>
<tr>
<td>Remote access permitted</td>
<td>Specifies whether this employee is permitted to log in on the terminal server with their user account.</td>
</tr>
<tr>
<td>Import data source</td>
<td>Specifies whether the employee can dial into the network with their user account.</td>
</tr>
<tr>
<td>Import data source</td>
<td>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.</td>
</tr>
<tr>
<td>Distinguished name</td>
<td>Distinguished name of the imported employee. This property should be set by the import.</td>
</tr>
<tr>
<td>Canonical name</td>
<td>Fully qualified name of the imported employee. This property should be set by the import.</td>
</tr>
</tbody>
</table>

**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 37: Configuration parameter for forming the central user accounts**

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| QER | Person | This configuration parameter specifies how the central user
Table 38: Example of forming of central user accounts

<table>
<thead>
<tr>
<th>First name</th>
<th>Last name</th>
<th>Central user account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clara</td>
<td>Harris</td>
<td>CLARA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HARRIS</td>
</tr>
<tr>
<td>Clara</td>
<td>Harris</td>
<td>CLARAH</td>
</tr>
<tr>
<td>Clara</td>
<td>Harrison</td>
<td>CLARAH1</td>
</tr>
</tbody>
</table>

Employee's central password

An employee’s central password can be used for logging into the target systems and for logging into 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 whether the configuration parameter QER | Person | UseCentralPassword is enabled. If not, set the configuration parameter.
- To use the central password of an employee for new user accounts belonging to the same employee, enable the QER | Person | UseCentralPassword | PermanentStore configuration parameter in Designer.

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, check in the Designer whether the configuration parameter QER | Person | UseCentralPassword | SyncToSystemPassword is set. If not, set the configuration parameter.

**NOTE:**

- The password policy **Employee central 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.
- 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 view QERPersonCentralPwdColumn. 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 column XMarkedForDeletion. 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 script QER_Publish_CentralPassword. For detailed information about editing scripts, see the One Identity Manager Configuration Guide.

**Related topics**

- Miscellaneous employee master data on page 86
- Password policies for employees on page 96
- Setting a secret password question on page 124
- Mutual aid on page 125

**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.
Set the configuration parameter in Designer 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 39: Configuration parameter for representing multiple identities

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person</td>
<td>MasterIdentity</td>
</tr>
</tbody>
</table>

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 the 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 40: Identity types**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary identity</td>
<td>Employee’s default identity. The employee has a default user account.</td>
</tr>
<tr>
<td>Organizational identity</td>
<td>Virtual employee (subidentity) for mapping different roles to an employee in the organization. The sub-identity has a user account of the type <strong>Organizational identity</strong>. Also enter a main identity.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Personalized admin identity</td>
<td>Virtual person (sub-identity) that belongs to a user account of the type <strong>Personalized administrator identity</strong>. Also enter a main identity.</td>
</tr>
<tr>
<td>Sponsored identity</td>
<td>Dummy employee who is linked to a user account of the type <strong>Sponsored identity</strong>. Assign a manager to the employee.</td>
</tr>
<tr>
<td>Shared identity</td>
<td>Dummy employee who is linked to an administrative user account of the type <strong>Shared identity</strong>. Assign a manager to the employee.</td>
</tr>
<tr>
<td>Service identity</td>
<td>Dummy employee who is linked to a user account of the type <strong>Service identity</strong>. Assign a manager to the employee.</td>
</tr>
</tbody>
</table>

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. Connect these sub-identities with the user account. This allows you to issue the required permissions to the various user accounts.

The sponsored identity, group identity, and service identity are dummy persons via 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 86
- Mapping multiple employee identities

**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

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 Designer. This schedule checks the start date for disabling and sets **Temporarily disabled** when it is reached.
- Configure the **Enable temporarily disabled accounts** schedule in Designer. 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 option **No inheritance** 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 Designer. This schedule regularly checks the leaving date and sets the option **Permanently disabled** 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. Select **Employees | Inactive employees**.
2. Select the employee in the result list.
3. Select **Re-enable employee**.
   An alert appears.
4. Confirm the security prompt with **Yes** if the employee should be enabled. Otherwise close the alert with **No**.

On the master data form for the employee, the option **Disabled permanently** is not set. The end date and last working day are deleted.

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 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 the delete delay has expired. You can configure an alternative deletion delay in the Person table in Designer.

**Related topics**

- Temporarily deactivating employees on page 94
- Permanently deactivating employees on page 94

---

**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 polices 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 user or customize if required. You can also define your own password policies.
Detailed information about this topic

- Predefined password policies on page 97
- Using a password policy on page 98
- Editing password policies on page 100
- Custom scripts for password requirements on page 103
- Defining the excluded list for passwords on page 106
- Checking a password on page 106
- Testing generation of a password 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 defined the settings for the system user passwords (DialogUser.Password and Person.DialogUserPassword) as well as the access code for a one off 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 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 password policy does not violate the 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 a password policy

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

The password policy that is applied for 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. Password policy 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 98
- 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 Manager, select the Employees | Basic configuration data | Password policies | Password policies category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Select the assignment you want to change in **Assignments**.
5. Select the new password policy to apply from the **Password Policies** menu.
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 via 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 Manager, select **Employees | Basic configuration data | Password policies| Password policies**.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply to</td>
<td>Application scope of the password policy.</td>
</tr>
</tbody>
</table>

**To specify an application scope**

a. Click ➔ next to the text box.

b. Under **Table**, select the table that contains the basic objects. You have the following options:
   - Departments (Department table)
   - Business roles (Org table)

   **NOTE**: This table is only available if Business Roles Module is installed.
   - Locations (Locality table)
   - Cost centers (Profitcenter table)

c. Under **Apply to**, select the specific department, cost center, location or business role.

d. Click **OK**.

<table>
<thead>
<tr>
<th>Password column</th>
<th>The password column's identifier. You have the following options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Employees - central password (table Employee, column CentralPassword)</td>
</tr>
<tr>
<td></td>
<td>• Employees - password (table Employee, column DialogUserPassword)</td>
</tr>
<tr>
<td></td>
<td>• Employees - access code (table Employee, column Passcode)</td>
</tr>
</tbody>
</table>

| Password policy | The identifier of the password policy to be used.                             |

5. Save the changes.

---

**Editing password policies**

**To edit a password policy**

1. In Manager, select the **Employees | Basic configuration data | Password policies** category.
2. Select the password policy in the result list and select **Change master data**.
3. Edit the password policy's master data.
4. Save the changes.
Detailed information about this topic

- General master data for a password policy on page 101
- Policy settings on page 101
- Character classes for passwords on page 102
- Custom scripts for password requirements on page 103

General master data for a password policy

Enter the following master data for a password policy.

Table 42: Master data for a password policy

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Password policy name. Translate the given text using the button.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation. Translate the given text using the button.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Custom error message outputted if the policy is not fulfilled. Translate the given text using the button.</td>
</tr>
<tr>
<td>Owner (Application Role)</td>
<td>Application roles whose members can configure the password policies.</td>
</tr>
<tr>
<td>Default policy</td>
<td>Mark as default policy for passwords.</td>
</tr>
</tbody>
</table>

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 43: Policy settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial password</td>
<td>Initial password for newly created employees. If a password is not entered or if a random password is not generated when a employee is created, the initial password is used.</td>
</tr>
<tr>
<td>Property</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password confirmation</td>
<td>Reconfirm password.</td>
</tr>
<tr>
<td>Minimum Length</td>
<td>Minimum length of the password. Specify the number of characters a password must have.</td>
</tr>
<tr>
<td>Max. length</td>
<td>Maximum length of the password. Specify the number of characters a password can have.</td>
</tr>
<tr>
<td>Max. errors</td>
<td>Maximum number of errors. Set the number of invalid passwords. Only taken into account when logging in to One Identity Manager. 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. You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. For more detailed information, see the One Identity Manager Web Portal User Guide.</td>
</tr>
<tr>
<td>Validity period</td>
<td>Maximum age of the password. Enter the length of time a password can be used before it expires.</td>
</tr>
<tr>
<td>Password history</td>
<td>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.</td>
</tr>
<tr>
<td>Minimum password strength</td>
<td>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.</td>
</tr>
<tr>
<td>Name properties denied</td>
<td>Specifies whether name properties are permitted or not permitted in the password. If this option is enabled, name properties are not permitted in passwords. The values of the columns for which the Contains name properties for password check option is set are taken into account. Adjust this option in the column definition in Designer. For more detailed information, see the One Identity Manager Configuration Guide.</td>
</tr>
</tbody>
</table>

### Character classes for passwords

Use the Character classes tab to specify which characters are permitted for a password.
### Table 44: Character classes for passwords

<table>
<thead>
<tr>
<th>Property</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min. number letters</td>
<td>Specifies the minimum number of alphabetical characters the password must contain.</td>
</tr>
<tr>
<td>Min. number lowercase</td>
<td>Specifies the minimum number of lowercase letters the password must contain.</td>
</tr>
<tr>
<td>Min. number uppercase</td>
<td>Specifies the minimum number of uppercase letters the password must contain.</td>
</tr>
<tr>
<td>Min. number digits</td>
<td>Specifies the minimum number of digits the password must contain.</td>
</tr>
<tr>
<td>Min. number special characters</td>
<td>Specifies the minimum number of special characters the password must contain.</td>
</tr>
<tr>
<td>Permitted special characters</td>
<td>List of permitted characters.</td>
</tr>
<tr>
<td>Max. identical characters in total</td>
<td>Maximum number of identical characters that can be present in the password in total.</td>
</tr>
<tr>
<td>Max. identical characters in succession</td>
<td>Maximum number of identical character that can be repeated after each other.</td>
</tr>
<tr>
<td>Denied special characters</td>
<td>List of characters, which are not permitted.</td>
</tr>
<tr>
<td>Lowercase not allowed</td>
<td>Specifies whether the password can contain lower case letters. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Uppercase not allowed</td>
<td>Specifies whether the password can contain upper case letters. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Digits not allowed</td>
<td>Specifies whether the password can contain digits. This setting is only applies when passwords are generated.</td>
</tr>
<tr>
<td>Special characters not allowed</td>
<td>Specifies whether the password can contain special characters. This setting is only applies when passwords are generated.</td>
</tr>
</tbody>
</table>

### Custom scripts for password requirements

You can implement custom scripts for testing and generating password 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 a password on page 104
- Script for generating a password on page 105

Script for checking a password

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

Syntax for 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 test

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

Example for a script for testing a password

A password cannot start with ? or !. 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. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
   a. In Manager, select the **Employees | Basic configuration data | Password policies | Password policies** category.
   b. Select the password policy in the result list.
   c. Select **Change master data**.
   d. Enter the name of the script to be used to check a password in the **Check script** input field on the **Scripts** tab.
   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**

```csharp
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 property Entity of the PasswordPolicy class.
```

**Example for a script to generate a password**

In random passwords, the script replaces the ? and ! characters, which are not permitted.

```csharp
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("_"))
```

To use a custom script for generating a password

1. Create your script in the category Script Library in the Designer.
2. Edit the password policy.
   a. In Manager, select the Employees | Basic configuration data | Password policies | Password policies category.
   b. Select the password policy in the result list.
   c. Select Change master data.
   d. Enter the name of the script to be used to generate a password in the Generating script input field on the Scripts tab.
   e. Save the changes.

Related topics
- Script for checking a password 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. Select Base Data | Security settings | Restricted passwords in Designer.
2. Create a new entry with Object | New an enter the term to excluded to the list.
3. Save the changes.

Checking a password

When you test a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.
To test whether a password conforms to the password policy

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

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 Manager, select the Employees | Basic configuration data | Password policies | Password policies category.
2. Select the password policy in the result list.
3. Select Change master data.
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 7 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 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 maximum number of failed logins, the employee or system user can no longer log on to One Identity Manager.

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

Passwords for locked employees and system users can be reset in the Password Reset Portal. For more detailed information, see the *One Identity Manager Web Portal User Guide*.

**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 One Identity Manager can log in through the Web Portal. This functionality can be used, for example, if external employees, such as contract workers, should be provided with temporary access to the One Identity Manager. These employee can log in to the Web Portal as new workers. New employee objects are added for them in the One Identity Manager database.

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

- In One Identity Manager, an employee with the following properties is created:
  - **Certification status:** New
  - **Disabled permanently:** Enabled
  - **No inheritance:** Enabled
If the configuration parameter **QER | Attestation | UserApproval** is enabled, the new employee is attested automatically.

To assign company resources to the employee or to ensure editing permissions in the 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 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 configuration parameter **QER | Attestation | UserApproval** is enabled.

### To change an employee’s certification status manually

1. To change the certification status of an active person, select Employees | Employees.
   - OR -
   To change the certification status of a permanently disabled employee, select Employees | Inactive employees.
2. Select the employee in the result list.
3. Select **Change certification status** in the task view.
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 option Permanently disabled 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.

- Assigning through Dynamic Roles
  Assignment through dynamic roles is a special case of indirect assignment. Dynamic roles are used to specify role memberships dynamically. Employees, devices, and workdesks are not permanently assigned to a role, just when they fulfill certain conditions. A check is performed regularly to assess which employees, devices, or workdesks fulfill these conditions. 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 45: Possible assignments of company resources to employees

<table>
<thead>
<tr>
<th>Company Resource</th>
<th>Direct assignment permitted</th>
<th>Indirect assignment permitted</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>System roles</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Subscribable reports</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Account definitions</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Groups of custom target systems</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Active Directory Groups</td>
<td>-</td>
<td>+</td>
<td>All the employee's user accounts are added to the associated application group, which permit application inheritance.</td>
</tr>
<tr>
<td>SharePoint Groups</td>
<td>-</td>
<td>+</td>
<td>All the employee's SharePoint user accounts are added to SharePoint groups.</td>
</tr>
<tr>
<td>SharePoint roles</td>
<td>-</td>
<td>+</td>
<td>All the employee's SharePoint user accounts are added to SharePoint roles.</td>
</tr>
<tr>
<td>LDAP Groups</td>
<td>-</td>
<td>+</td>
<td>All the employee's LDAP user accounts, which permit group inheritance, are added to LDAP groups.</td>
</tr>
<tr>
<td>Notes Groups</td>
<td>-</td>
<td>+</td>
<td>All the employee's Notes user accounts are added to Notes groups.</td>
</tr>
<tr>
<td>SAP Groups</td>
<td>+</td>
<td>+</td>
<td>All the employee's SAP user accounts, which are in the same SAP clients, are added to SAP groups.</td>
</tr>
<tr>
<td>SAP profiles</td>
<td>+</td>
<td>+</td>
<td>All the employee's SAP user accounts, which are in the same SAP clients, are added to SAP profiles.</td>
</tr>
<tr>
<td>Company Resource</td>
<td>Direct assignment permitted</td>
<td>Indirect assignment permitted</td>
<td>Comment</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------</td>
<td>-------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>SAP roles</td>
<td>+</td>
<td>+</td>
<td>All the employee's SAP user accounts, which are in the same SAP clients, are added to SAP roles.</td>
</tr>
<tr>
<td>Structural profiles</td>
<td>-</td>
<td>+</td>
<td>All the employee's SAP user accounts, which are in the same SAP clients, are added to structural profiles.</td>
</tr>
<tr>
<td>BI analysis authorizations</td>
<td>-</td>
<td>+</td>
<td>All the employee's BI user accounts, which are in the same system, obtain BI analysis authorizations.</td>
</tr>
<tr>
<td>E-Business Suite entitlements</td>
<td>-</td>
<td>+</td>
<td>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.</td>
</tr>
<tr>
<td>Azure Active Directory Groups</td>
<td>-</td>
<td>+</td>
<td>All the employee's Azure Active Directory user accounts, which permit group inheritance, are added to Azure Active Directory groups.</td>
</tr>
<tr>
<td>Azure Active Directory administrator roles</td>
<td>-</td>
<td>+</td>
<td>All the employee's Azure Active Directory user accounts, which permit group inheritance, are added to Azure Active Directory administrator roles.</td>
</tr>
<tr>
<td>Azure Active Directory Subscriptions</td>
<td>-</td>
<td>+</td>
<td>All the employee's Azure Active Directory user accounts, which permit group inheritance, are given Azure Active Directory subscriptions.</td>
</tr>
<tr>
<td>Disabled Azure Active Directory service plans</td>
<td>-</td>
<td>+</td>
<td>All the employee's Azure Active Directory user accounts, which permit group inheritance, are given Azure Active Directory service plans.</td>
</tr>
<tr>
<td>Unix Groups</td>
<td>-</td>
<td>+</td>
<td>All the employee's Unix user accounts, which permit group inheritance, are added to Unix groups.</td>
</tr>
<tr>
<td>PAM user groups</td>
<td>-</td>
<td>+</td>
<td>All the employee's PAM user accounts for which the inheritance of groups is permitted are added to the PAM user groups.</td>
</tr>
</tbody>
</table>
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 24

Related topics

- Possible assignments of company resources through roles on page 22
- 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 65

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. Select the Employees | Employees.
2. Select the employee in the result list.
3. Select Assign organizations.
4. Assign organizations in Add assignments.
   - Assign departments on the Departments tab.
   - Assign locations on the Locations tab.
   - Assign cost centers on the Cost centers tab.

   **TIP:** In the Remove assignments area, you can remove the assignment of 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. Select the Employees | Employees.
2. Select the employee in the result list.
3. Select Change master data.
4. Adjust the following master data:
   - 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 65
- 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 user 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. Select the Employees | Employees.
2. Select the employee in the result list.
3. Select Assign business roles in the task view.
4. Assign business roles in **Add assignments**.

   **TIP:** In the **Remove assignments** area, you can remove the assignment of 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. Select the **Employees | Employees**.
2. Select the employee in the result list.
3. Select **Change master data**.
4. Enter the primary 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 detailed information, see the *One Identity Manager IT Shop Administration Guide*.

**To add an employee to the IT Shop**

1. Select the **Employees | Employees**.
2. Select the employee in the result list.
3. Select **Assign IT Shop memberships** in the task view.
4. Assign the custom nodes in **Add assignments**.
   - OR -
     Remove the custom nodes in **Remove assignments**.
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 | Birth-right Assignments** are automatically assigned to employees. Do not make any manually assignments to these application roles.

### To assign application to an employee

1. Select the **Employees | Employees**.
2. Select the employee in the result list.
3. Select **One Identity Manager Assign application roles**.
4. Assign the application roles in **Add assignments**.
   - OR -
   Remove the application roles in **Remove assignments**.
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. Select the **Employees | Employees**.
2. Select the employee to whom the resources will be assigned, from the result list.
3. Select **Assign resources** in the task view.
4. Assign resources in **Add assignments**.
   - OR -
   Remove the resources in **Remove assignments**.
5. Save the changes.

### Related topics

- Assigning resources directly to employees on page 171
- Managing resources on page 164
Assigning applications directly to employees

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

You can assign applications directly or indirectly to employees. Indirect assignment is carried out by assigning employees and applications to company structures, such as departments, cost centers, locations, or business roles. For detailed information about working with applications, see One Identity Manager Application Management Administration Guide.

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

To assign an application directly to an employee

1. Select the Employees | Employees.
2. Select the employee to whom the application will be assigned from the results list.
3. Select Assign applications in the task view.
4. Assign applications in Add assignments.
   - OR -
   Remove applications in Remove assignments.
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. Select the Employees | Employees.
2. Select the employee in the result list.
3. Select Assign system roles.
4. Assign system roles in **Add assignments**.

   **TIP:** In the **Remove assignments** area, you can remove the assignment of 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 more 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. Select the **Employees | Employees**.
2. Select the employee in the result list.
3. Select **Assign subscribable reports** in the task view.
4. Assign reports in **Add assignments**.

   **TIP:** You can remove the assignment of reports in the **Remove assignments** area.

   **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 a 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, activate the configuration parameter **SysConfig | Display | SourceDetective** and compile the database.

**To display the origin of an employee's entitlements**

1. Select the **Employees | Employees**.
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 employee 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 report **Overview of all assignments**.
- 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 employee for tracking. This creates a new business role to which the employees are assigned.
### Table 46: Meaning of Icons in the Report Toolbar

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>📁</td>
<td>Show the legend with the meaning of the report control elements</td>
</tr>
<tr>
<td>✨</td>
<td>Saves the current report view as a graphic.</td>
</tr>
<tr>
<td>🏛</td>
<td>Selects the role class used to generate the report.</td>
</tr>
<tr>
<td>🧩</td>
<td>Displays all roles or only the affected roles.</td>
</tr>
</tbody>
</table>

### 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. Select the **Employees | Employees**.
2. Select the employee in the result list.
3. Select **Employee overview** in the task view.
   
   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 **Employee entitlements overview** in the task view.
   
   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. Select the Employees | Employees.
2. Select the employee in the result list.
3. Select Show calls in the task view to display calls entered for an employee.
4. Select New call in the task view, to enter a new call.
5. Save the changes.

Assigning extended properties

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.
To specify extended properties for a group

1. Select the Employees | Employees.
2. Select the employee in the result list.
3. Select Assign extended properties in the task view.
4. Assign extended properties in Add assignments.

   **TIP:** In the Remove assignments area, you can remove the assignment of extended properties.

   To remove an assignment
   - Select the extended property and double click ☑.

5. Save the changes.

Related topics
- Edit extended properties on page 181

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 Change security question in the task view.
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 Mutual aid - set password in the task view.

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 recipient's 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 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 configuration parameter Common | MailNotification | DefaultCulture.
   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 area (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 area 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.
5. State of primary department.
6. Country of primary department.
7. State of primary cost center.
11. Fallback, in case the area 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 47: Employee reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlement Origins</td>
<td>The report shows an employee's entitlements and roles and the possible assignment methods.</td>
</tr>
<tr>
<td>Request History</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Data quality of supervised employees</td>
<td>This report evaluates the data quality of employee data records. All employees under supervision are taken into account.</td>
</tr>
<tr>
<td>Employees per department</td>
<td>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.</td>
</tr>
<tr>
<td>Employees per cost center</td>
<td>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.</td>
</tr>
<tr>
<td>Employees per location</td>
<td>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.</td>
</tr>
<tr>
<td>Data quality summary for employee records</td>
<td>The report contains different analyzes of data quality for all employees. You can find this report in My One Identity Manager.</td>
</tr>
</tbody>
</table>
Related topics

- Displaying the origin of an employee's roles and entitlements on page 119
- Analyzing role memberships and employee assignments on page 121
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

- Set the configuration parameter "Hardware" in the Designer 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. You can find an overview of all configuration parameters in **Base data | General | Configuration parameters** in Designer.

- **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
- **Appendix: Configuration parameters for managing devices and workdesks** on page 190

**Device models**

The prerequisite for adding hardware 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 hardware model**

1. Select the category **Devices & Workdesks | Basic configuration data | Device models**.
2. Select a device model in the result list. Select **Change master data**.
   - 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 48: Device model master data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device model</td>
<td>Name of the device model.</td>
</tr>
<tr>
<td>Device type</td>
<td>Type of the device. During the setup of new device, the device model’s</td>
</tr>
<tr>
<td></td>
<td>device type filters the forms that are available for handling master data.</td>
</tr>
<tr>
<td>Company</td>
<td>Name of manufacturer. Use the next to the text box to add a new company.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <strong>Business partners</strong> on page 134.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only the companies that are marked as manufacturers can be</td>
</tr>
<tr>
<td></td>
<td>selected. When a new device is added, the company named as</td>
</tr>
<tr>
<td></td>
<td>manufacturer in the device model is used for the device.</td>
</tr>
<tr>
<td>Service item</td>
<td>If you assigned a service item to the device model, the usage of the</td>
</tr>
<tr>
<td></td>
<td>device model can be booked internally. Use the next to the text box to add</td>
</tr>
<tr>
<td></td>
<td>a new service item.</td>
</tr>
<tr>
<td>Website</td>
<td>Manufacturers Website.</td>
</tr>
<tr>
<td></td>
<td>Use the <strong>Browse</strong> task to see the manufacturer’s website in the standard</td>
</tr>
<tr>
<td></td>
<td>web browser.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Additional data</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PC</td>
<td>Specifies whether, in principle, the device can be used as a PC in the sense</td>
</tr>
<tr>
<td></td>
<td>of workstation.</td>
</tr>
<tr>
<td>Server</td>
<td>Specifies whether the device is used as a server.</td>
</tr>
<tr>
<td>Local peripheral</td>
<td>Specifies whether this device type is a local peripheral to attach to a PC.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Specifies whether the device model is in use or not.</td>
</tr>
</tbody>
</table>

**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 49: Inventory data for a device model

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default supplier</td>
<td>Name of supplier. For more information, see Business partners on page 134.</td>
</tr>
<tr>
<td>Employee</td>
<td>Employee responsible for the purchase.</td>
</tr>
<tr>
<td>Alternative device model</td>
<td>Alternative device model.</td>
</tr>
<tr>
<td>Warranty [months]</td>
<td>Standard manufacturer warranty in months.</td>
</tr>
<tr>
<td>Additional guarantee [months]</td>
<td>Additional manufacturer guarantee in months.</td>
</tr>
<tr>
<td>Usage [months]</td>
<td>Estimated period of use.</td>
</tr>
<tr>
<td>Minimum stock</td>
<td>Minimum level of stock in storage.</td>
</tr>
<tr>
<td>Maximum stock</td>
<td>Maximum level of stock in storage.</td>
</tr>
<tr>
<td>Item number</td>
<td>Article number at suppliers.</td>
</tr>
<tr>
<td>Request units</td>
<td>Measurement units for requests.</td>
</tr>
<tr>
<td>Minimum request quantity</td>
<td>Minimum quantity for requests.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Last quote date</td>
<td>Last quote date.</td>
</tr>
<tr>
<td>Price of last offer</td>
<td>Price of last offer.</td>
</tr>
<tr>
<td>Last delivery date</td>
<td>Last delivery date.</td>
</tr>
<tr>
<td>Price of last delivery</td>
<td>Price of last delivery.</td>
</tr>
</tbody>
</table>

**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 Change master data.
   - 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 50: General master data for a company**

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leasing partner</td>
<td>Specifies whether this is a leasing provider or rental firm.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Specifies whether this is a manufacturer.</td>
</tr>
<tr>
<td>Remarks</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

### Table 51: Company address

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Street</td>
<td>Street or road.</td>
</tr>
<tr>
<td>Building</td>
<td>Building</td>
</tr>
<tr>
<td>Zip code</td>
<td>Zip code.</td>
</tr>
<tr>
<td>City</td>
<td>City.</td>
</tr>
<tr>
<td>State</td>
<td>State.</td>
</tr>
<tr>
<td>Country</td>
<td>Country.</td>
</tr>
<tr>
<td>Phone</td>
<td>Company's telephone number.</td>
</tr>
<tr>
<td>Fax</td>
<td>Company's fax number.</td>
</tr>
<tr>
<td>Email address</td>
<td>Company's email address.</td>
</tr>
<tr>
<td>Website</td>
<td>Company's website.</td>
</tr>
</tbody>
</table>

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 **Hardware & Workdesks | Basic configuration data | Device status** category.
2. Select a device status in the result list. Select **Change master data**.
   - 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 52: Device status general data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device status</td>
<td>Name of the device status.</td>
</tr>
<tr>
<td>Short description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

### 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 **Change master data**.
   - 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 53: Master data for a workdesk

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Workdesk status name.</td>
</tr>
<tr>
<td>Short description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

### 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 **Change master data**.
   - 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 54: Master data for a workdesk type**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workdesk type</td>
<td>Workdesk status name.</td>
</tr>
<tr>
<td>Display name</td>
<td>Name for displaying in the One Identity Manager tools.</td>
</tr>
<tr>
<td>Short description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Leasing fee</td>
<td>Leasing fee.</td>
</tr>
<tr>
<td>Floppy disk drive required</td>
<td>Specifies whether this workdesk type requires a floppy disk drive.</td>
</tr>
<tr>
<td>CD-ROM drive required</td>
<td>Specifies whether this workdesk type requires a CD-ROM drive.</td>
</tr>
</tbody>
</table>

### Setting up a device

**Table 55: Configuration parameter for setting up a device**

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>Effect when set</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Workdesk</td>
</tr>
</tbody>
</table>

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

**To edit a device**

1. Select **Devices & Workdesks | Devices**.
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 **Change master data**.
   - 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 56: General Master Data for Devices

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset number</td>
<td>Number of the asset in the bookkeeping.</td>
</tr>
<tr>
<td>Device ID</td>
<td>Unique device ID.</td>
</tr>
<tr>
<td>PC</td>
<td>Specifies whether the hardware is a computer.</td>
</tr>
<tr>
<td>Server</td>
<td>Specifies whether the hardware is a server.</td>
</tr>
<tr>
<td>Local periphery</td>
<td>Specifies whether this is a local periphery, for example, monitor, printer, or other periphery device.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Name of manufacturer.</td>
</tr>
<tr>
<td>Device model</td>
<td>Name of the device model. The master data available depends on the selected device model.</td>
</tr>
<tr>
<td>Device status</td>
<td>Device's status.</td>
</tr>
<tr>
<td>Workdesk</td>
<td>The device's workdesk. This workdesk is used to assign various devices to a workstation or a server. If the &quot;Hardware</td>
</tr>
<tr>
<td>Parent device</td>
<td>A parent device which is linked to this device.</td>
</tr>
<tr>
<td>VM Client (option)</td>
<td>Specifies whether this device is a virtual machine.</td>
</tr>
<tr>
<td>VM Host</td>
<td>Device on which a virtual machine is installed. The selection is shared if the VM client is set.</td>
</tr>
<tr>
<td>VM Host (option)</td>
<td>Specifies whether this hardware is host for a virtual machine.</td>
</tr>
<tr>
<td>Phone</td>
<td>Telephone number.</td>
</tr>
<tr>
<td>Used by</td>
<td>Employee who uses this device.</td>
</tr>
<tr>
<td>Primary department</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Primary location    | Location to which the device is primary assigned. Company resources can be inherited by a device through these primary assignments if One
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Manager</td>
<td>Identity Manager is appropriately configured.</td>
</tr>
<tr>
<td>Primary cost center</td>
<td>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.</td>
</tr>
<tr>
<td>Primary business roles</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This property is available if the Business Roles Module is installed.</td>
</tr>
<tr>
<td>Investment</td>
<td>Investments or investment plans for the device.</td>
</tr>
<tr>
<td>Location description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Remarks</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>No inheritance</td>
<td>Specifies whether the device inherits company resources through roles. If this option is set, the employee cannot inherit. Direct assignments remain intact.</td>
</tr>
<tr>
<td>Operating system</td>
<td>Operating system identifier.</td>
</tr>
<tr>
<td>Operating system version</td>
<td>Version number of the operating system.</td>
</tr>
<tr>
<td>Service pack operating system</td>
<td>Service pack identifier.</td>
</tr>
<tr>
<td>Hotfix operating system</td>
<td>Hotfix identifier.</td>
</tr>
<tr>
<td>Carrier</td>
<td>Carrier contract for the device.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Manufacturer's serial number.</td>
</tr>
<tr>
<td>MAC address</td>
<td>The device's MAC address.</td>
</tr>
<tr>
<td>IMEI</td>
<td>The device's IMEI number.</td>
</tr>
<tr>
<td>ICCID</td>
<td>The device's ICCID number.</td>
</tr>
<tr>
<td>BIOS version</td>
<td>Version of the BIOS.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RAM [MB]</td>
<td>RAM in megabytes.</td>
</tr>
<tr>
<td>HDD capacity [MB]</td>
<td>Capacity of the first disk in megabytes</td>
</tr>
<tr>
<td>Second HDD capacity [MB]</td>
<td>Capacity of the second disk in megabytes</td>
</tr>
<tr>
<td>Max. vertical resolution</td>
<td>Maximum vertical image resolution.</td>
</tr>
<tr>
<td>Max. horizontal resolution</td>
<td>Maximum horizontal image resolution.</td>
</tr>
<tr>
<td>Import data source</td>
<td>Target system or data source, from which the data set was imported.</td>
</tr>
<tr>
<td>Spare field no. 01 ...</td>
<td>Additional company specific information. Use Designer to customize</td>
</tr>
<tr>
<td>Spare field no. 10</td>
<td>display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

**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 159
- [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 57: Network data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address in IPv4 format.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>address (IPv4)</td>
<td>IP address in IPv6 format.</td>
</tr>
<tr>
<td>IP address (IPv6)</td>
<td>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.</td>
</tr>
<tr>
<td>Use DHCP</td>
<td>Specifies whether WINS name resolution is used. If this option is set, enter the IP addresses of the preferred and the alternative WINS server.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Subnet mask.</td>
</tr>
<tr>
<td>Default gateway</td>
<td>Default gateway.</td>
</tr>
<tr>
<td>Use WINS</td>
<td>IP address of the preferred WINS server.</td>
</tr>
<tr>
<td>WINS primary</td>
<td>IP address of the alternative WINS server.</td>
</tr>
<tr>
<td>WINS secondary</td>
<td>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 sever cannot be found. Normally, this input should be left empty.</td>
</tr>
<tr>
<td>Range ID</td>
<td>Specifies whether DNS name resolution is used. If this option is set, enter the IP address of the preferred and the alternative DNS server.</td>
</tr>
<tr>
<td>Use DNS</td>
<td>IP address of the preferred DNS server.</td>
</tr>
<tr>
<td>DNS server</td>
<td>IP address of the alternative DNS server.</td>
</tr>
<tr>
<td>2. DNS server</td>
<td>IP address of the alternative DNS server.</td>
</tr>
<tr>
<td>3. DNS server</td>
<td>IP address of the alternative DNS server.</td>
</tr>
<tr>
<td>DNS name</td>
<td>Suffix of DNS domain the device belongs to.</td>
</tr>
<tr>
<td>DNS host name</td>
<td>DNS name of the computer.</td>
</tr>
<tr>
<td>Remote boot</td>
<td>Specifies whether this device uses remote booting. The property is available if the &quot;Hardware</td>
</tr>
<tr>
<td>Remote boot type</td>
<td>Data for the remote boot type. The property is available if the &quot;Hardware</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Company resources</th>
<th>Direct assignment permitted</th>
<th>Indirect assignment permitted</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory groups</td>
<td>-</td>
<td>+</td>
<td>All Active Directory computers that reference this device are added to Active Directory groups.</td>
</tr>
<tr>
<td>LDAP groups</td>
<td>-</td>
<td>+</td>
<td>All LDAP computers that reference this device are added to LDAP groups.</td>
</tr>
</tbody>
</table>

**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 24

Related topics

- Possible assignments of company resources through roles on page 22
- 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 151
- Working with dynamic roles on page 65

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 Assign organizations.
4. Assign organizations in Add assignments.
   - Assign departments on the Departments tab.
   - Assign locations on the Locations tab.
   - Assign cost centers on the Cost centers tab.

   TIP: In the Remove assignments area, you can remove the assignment of 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 Change master data.
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 65
- 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 user 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 Assign business roles in the task view.
4. Assign business roles in **Add assignments**.

   **TIP:** In the **Remove assignments** area, you can remove the assignment of 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 **Change master data**.
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 **Device overview**.
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 **Show calls** in the task view to display calls entered for a device.
5. Select **New call** in the task view, 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 59: Configuration parameters for setting up workdesk

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Effect when set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Workdesk</td>
</tr>
</tbody>
</table>

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, activate the “Hardware | Workdesk | WorkdeskAuto” configuration parameter in the Designer.
To edit a workdesk

1. Select the category Devices & Workdesks | Workdesks | Names.
2. Select a workdesk in the result list. Select Change master data.
   - 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 151
- Appendix: Configuration parameters for managing devices and workdesks on page 190

General master data for a workdesk

Enter the following general master data for a workdesk.

Table 60: General Master Data for a Workdesk

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workdesk</td>
<td>Workdesk name. If the &quot;Hardware</td>
</tr>
<tr>
<td>Workdesk type</td>
<td>Type of the workdesk.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the workdesk.</td>
</tr>
<tr>
<td>Operating system</td>
<td>Workdesk's operating system.</td>
</tr>
<tr>
<td>Display name</td>
<td>The display name is used to display the workdesk in the One Identity Manager tools user interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Primary cost center</td>
<td>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.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Primary business roles</td>
<td>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.</td>
</tr>
<tr>
<td>Installation date</td>
<td>Date of going into operation.</td>
</tr>
<tr>
<td>Workdesk supervisor</td>
<td>Employee responsible for this workdesk.</td>
</tr>
<tr>
<td>Checked by</td>
<td>Employee who checked this workdesk.</td>
</tr>
<tr>
<td>Date checked</td>
<td>Last time the workdesk was checked.</td>
</tr>
<tr>
<td>Check remarks</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Service type</td>
<td>Information about the service done on this workdesk, for example, internal or external service provider.</td>
</tr>
<tr>
<td>Corresponding service agreements set up</td>
<td>Specifies whether the workdesk is set up corresponding to service agreements.</td>
</tr>
<tr>
<td>No inheritance</td>
<td>Specifies whether the workdesk inherits company resources through roles. If this option is set, the employee cannot inherit. Direct assignments remain intact.</td>
</tr>
<tr>
<td>Spare field no. 01 ... Spare field no. 10</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

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 61: Workdesk Location Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary department</td>
<td>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.</td>
</tr>
<tr>
<td>Primary location</td>
<td>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.</td>
</tr>
<tr>
<td>Fax</td>
<td>Fax number.</td>
</tr>
<tr>
<td>Remarks (fax)</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Building</td>
<td>Building</td>
</tr>
<tr>
<td>Room</td>
<td>Room.</td>
</tr>
<tr>
<td>Phone</td>
<td>Telephone number.</td>
</tr>
<tr>
<td>Floor</td>
<td>Floor.</td>
</tr>
<tr>
<td>Remarks (room)</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

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 62: Miscellaneous workdesk data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup date</td>
<td>Date of going into operation.</td>
</tr>
<tr>
<td>Withdrawal date</td>
<td>Date on which the workdesk is written off.</td>
</tr>
<tr>
<td>Leasing fee</td>
<td>Leasing fee.</td>
</tr>
<tr>
<td>Floppy disk drive required</td>
<td>Specifies whether this workdesk requires a floppy disk drive.</td>
</tr>
<tr>
<td>CD-ROM drive required</td>
<td>Specifies whether this workdesk requires a CD-ROM drive.</td>
</tr>
<tr>
<td>Comment</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>
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 the One Identity Manager modules and are not available until the modules are installed.

<table>
<thead>
<tr>
<th>Company Resource</th>
<th>Direct assignment permitted</th>
<th>Indirect assignment permitted</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>System roles</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td>+</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Active Directory groups</td>
<td>-</td>
<td>+</td>
<td>All Active Directory computers that reference the workdesk device are added to Active Directory groups.</td>
</tr>
</tbody>
</table>
### Company Resource Direct assignment permitted Indirect assignment permitted Remarks

| 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 24

### Related topics

- Possible assignments of company resources through roles on page 22
- 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 65

### 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 category **Devices & Workdesks | Workdesks | Names**.
2. Select the workdesk in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost centers** tab.
In the **Remove assignments** area, you can remove the assignment of 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 category **Devices & Workdesks | Workdesks | Names**.
2. Select the workdesk in the result list.
3. Select **Change master data**.
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 151
- Assigning company resources to departments, cost centers, and locations on page 52
- Working with dynamic roles on page 65
- 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 user the corresponding business role tasks.

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

1. Select the category **Devices & Workdesks | Workdesks | Names**.
2. Select the workdesk in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   **TIP:** In the **Remove assignments** area, you can remove the assignment of 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 category **Devices & Workdesks | Workdesks | Names**.
2. Select the workdesk in the result list.
3. Select **Change master data**.
4. Enter the primary role.
5. Save the changes.

**Related topics**

- Assigning company resources to workdesks on page 151
- One Identity Manager Business Roles Administration Guide

### Assigning applications directly to workdesks

You can assign applications directly or indirectly to a workdesk. Indirect assignment is carried out by allocating the workdesk and applications in company structures, such as departments, cost centers, locations, or business roles.

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

**To assign applications to a workdesk**

1. Select the category **Devices & Workdesks | Workdesks | Names**.
2. Select the workdesk in the result list.
3. Select **Assign applications** in the task view, to assign application directly to the workdesk.
4. Assign applications in **Add assignments**.
   - OR -
   Remove applications in **Remove assignments**.
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 category **Devices & Workdesks | Workdesks | Names**.
2. Select the workdesk in the result list.
3. Select **Assign system roles** in the task view, to assign system roles directly to the workdesk.
4. Assign system roles in **Add assignments**.

   **TIP:** In the **Remove assignments** area, you can remove the assignment of 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 category Devices & Workdesks | Workdesks | Names.
2. Select the workdesk in the result list.
3. Select Workdesk overview in the task view.

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 category Devices & Workdesks | Workdesks | Names.
2. Select the workdesk in the result list.
3. Select the task Assign devices.
4. Assign the devices in Add assignments.
   - OR -
   In the Remove assignments area, 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 category Devices & Workdesks | Workdesks | Names.
2. Select the workdesk in the result list.
3. Select **Assign employees** in the task view.
4. Assign employees in **Add assignments**.
   - OR -
   Remove employees from **Remove assignments**.
5. Save the changes.

**Related topics**
- General employee master data on page 80

**Assigning service agreements and enter calls**

Installed modules:  Helpdesk Module

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

**To enter help desk data for a workdesk**

1. Select the category **Devices & Workdesks | Workdesks | Names**.
2. Select the workdesk in the result list.
3. Select the **Assign service agreements** task to assign the valid service agreements to the workdesk.
   The service agreements are taken into account when calculating solution and reaction times in the case of a help desk call for this workdesk.
4. Select **Show calls**, to show the calls entered for a workdesk.
5. Select **New call** in the task view, to enter a new call.
6. Save the changes.

**Related topics**
- One Identity Manager Help Desk Module User Guide

**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**
- Enable the "Hardware | AssetAccounting" configuration parameter in the Designer and compile the database.

**Detailed information about this topic**
- Basic data for asset management on page 158
- Entering investments and investment plans on page 159
- Editing device asset data on page 160

## 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 158
- Asset types on page 159
- Basic data for device admin on page 130
- Appendix: Configuration parameters for managing devices and workdesks on page 190

### 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 Change master data.
   - 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 64: Asset class master data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage class</td>
<td>Description of the asset class.</td>
</tr>
<tr>
<td>Display name</td>
<td>Name for displaying in the One Identity Manager tools.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

**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 Change master data.
   - 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 then to devices.

**To edit an investment**

1. Select the Devices & Workdesks | Investments category.
2. Select an investment in the result list. Select Change master data.
   - OR -
   Click in the result list.
3. Edit the following master data.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investment</td>
<td>Investment project name.</td>
</tr>
<tr>
<td>Date</td>
<td>Investment date.</td>
</tr>
<tr>
<td>Investment manager</td>
<td>The employee responsible for this investment.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Remarks</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

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 Edit asset data.
4. Save the changes.

Detailed information about this topic
- Master data for asset data on page 160
- Commercial data on page 162

Master data for asset data

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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset number</td>
<td>Number of the asset in the bookkeeping.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Asset</td>
<td>Asset.</td>
</tr>
<tr>
<td>Storage class</td>
<td>Asset class.</td>
</tr>
<tr>
<td>Storage type</td>
<td>Asset type.</td>
</tr>
<tr>
<td>Device status</td>
<td>The device's status.</td>
</tr>
<tr>
<td>Enabling</td>
<td>Date for enabling the asset or beginning the lease, respectively.</td>
</tr>
<tr>
<td>Deactivation</td>
<td>Date for disabling the asset or end of lease, respectively.</td>
</tr>
<tr>
<td>Replacement value</td>
<td>Value for replacing with a new device.</td>
</tr>
<tr>
<td>Depreciated value</td>
<td>Depreciation value for the device.</td>
</tr>
<tr>
<td>Company owned</td>
<td>Specifies whether or not the device is owned by the company.</td>
</tr>
<tr>
<td>Leased</td>
<td>Specifies whether the device is leased.</td>
</tr>
<tr>
<td>Invoice number</td>
<td>Invoice number of the purchase.</td>
</tr>
<tr>
<td>PSP character string</td>
<td>Asset PSP as character string.</td>
</tr>
<tr>
<td>Last inventory run</td>
<td>Date of last inventory.</td>
</tr>
<tr>
<td>Primary cost center</td>
<td>Cost center. Company resources can be inherited by a device through these primary assignments if One Identity Manager is appropriately configured.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Serial number of the device.</td>
</tr>
<tr>
<td>Delivery remarks</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Inventory remarks</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Primary location</td>
<td>Location. Company resources can be inherited by a device through these primary assignments if One Identity Manager is appropriately configured.</td>
</tr>
<tr>
<td>Primary department</td>
<td>Department. Company resources can be inherited by a device through these primary assignments if One Identity Manager is appropriately configured.</td>
</tr>
</tbody>
</table>
Related topics

- Asset classes on page 158
- Asset types on page 159
- 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 Designer.

Table 67: Device asset data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition date</td>
<td>Date of purchase.</td>
</tr>
<tr>
<td>Delivery date</td>
<td>Date of delivery.</td>
</tr>
<tr>
<td>Delivery voucher number</td>
<td>Delivery voucher number.</td>
</tr>
<tr>
<td>Warranty</td>
<td>Warranty expiry date.</td>
</tr>
<tr>
<td>Warranty number</td>
<td>Warranty number.</td>
</tr>
<tr>
<td>Setup date</td>
<td>Date of going into operation.</td>
</tr>
<tr>
<td>Owner</td>
<td>Leasing company.</td>
</tr>
<tr>
<td>Supplier</td>
<td>Name of supplier.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Name of manufacturer.</td>
</tr>
<tr>
<td>Purchase price</td>
<td>Purchase price.</td>
</tr>
<tr>
<td>Internal price</td>
<td>Internal price.</td>
</tr>
<tr>
<td>Sales price</td>
<td>Sales price.</td>
</tr>
<tr>
<td>Currency</td>
<td>Currency unit</td>
</tr>
<tr>
<td>Inventory note</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Withdrawal date</td>
<td>Date for writing off the device.</td>
</tr>
<tr>
<td>Leasing fee</td>
<td>Leasing fee.</td>
</tr>
<tr>
<td>Internal transfer price</td>
<td>Internal transfer price.</td>
</tr>
<tr>
<td>Depreciation month</td>
<td>Depreciation in months</td>
</tr>
</tbody>
</table>
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 68: Resource Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>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</td>
<td>QERResource</td>
</tr>
<tr>
<td>Multi-request resources</td>
<td>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.</td>
<td>QERReuse</td>
</tr>
<tr>
<td>Multi-requestable/unsubscribable resources</td>
<td>Resources which 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.</td>
<td>QERReuseUS</td>
</tr>
</tbody>
</table>
They remain assigned until the request is canceled.
Example: printer, monitor

Detailed information about this topic

- Editing resources on page 168
- Assigning resources to employees on page 170
- Editing multi-request resources on page 175
- Assigning multi-request resources to employees on page 176
- Reports about resources on page 178

One Identity Manager users for managing resources

The following users are used for user administration.

Table 69: User

<table>
<thead>
<tr>
<th>User</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators for the IT Shop</td>
<td>Administrators must be assigned to the Request &amp; Fulfillment</td>
</tr>
<tr>
<td></td>
<td>Users with this application role:</td>
</tr>
<tr>
<td></td>
<td>- Edit the resources and assign them to IT Shop structures and</td>
</tr>
<tr>
<td></td>
<td>employees.</td>
</tr>
<tr>
<td>One Identity Manager</td>
<td>Create customized permissions groups for application roles</td>
</tr>
<tr>
<td>Manager administrators</td>
<td>for role-based login to administration tools in Designer as required.</td>
</tr>
<tr>
<td></td>
<td>Create system users and permissions groups for non-role-based login to</td>
</tr>
<tr>
<td></td>
<td>administration tools in Designer as required.</td>
</tr>
<tr>
<td></td>
<td>Enable or disable additional configuration parameters in Designer</td>
</tr>
<tr>
<td></td>
<td>as required.</td>
</tr>
<tr>
<td></td>
<td>Create custom processes in Designer as required.</td>
</tr>
<tr>
<td></td>
<td>Create and configures schedules as required.</td>
</tr>
<tr>
<td></td>
<td>Create and configure password policies as required.</td>
</tr>
</tbody>
</table>
Basic data for resources

The following basic data is required for managing resources.

- **Resource Types**
  You can use resource types to group resources.

- **Processing status**
  Processes statuses pass on the status of single approval steps. You can set the processing status for each approval step in the approval workflow depending on whether the approval decision was negative or positive. Depending on the result of the approval decision, the appropriate processing status is set for the request.

- **Extended properties**
  Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

Detailed information about this topic

- Resource types on page 166
- Processing status on page 166
- Edit extended properties on page 181

Resource types

You can use resource types to group resources.

**To define resource types**

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

Processing status

Processes statuses pass on the status of single approval steps. You can set the processing status for each approval step in the approval workflow depending on whether the approval
decision was negative or positive. Depending on the result of the approval decision, the appropriate processing status is set for the request.

**NOTE:** Manual post-processing of resource requests is not part of the standard One Identity Manager installation. Implement a custom solution for the required functionality.

**Example**

An employee requests a mobile phone through the IT Shop. This request is authorized by the person in charge of the employee’s cost center. The following steps could be necessary:

1. Initiate phone request at the dealers
2. Check delivery
3. Activate the resource in asset accounting
4. Deliver phone to employee

Once a processing step has been completed the processing status for the assigned resource should be updated. Employees can use this to keep up-to-date with the progress of their requests.

**To edit processing statuses**

1. Select Entitlements | Basic configuration data | Processing status.
2. Select a processing status in the result list. Select Change master data.
   - OR –
     Click 🔄 in the result list.
3. Edit the processing status’s master data.
4. Save the changes.

Enter the following properties for a processing status.

**Table 70: General master data for a processing status**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing status</td>
<td>Name of the processing status.</td>
</tr>
<tr>
<td>Success</td>
<td>The processing status marks the success of the processing step.</td>
</tr>
<tr>
<td>Closed</td>
<td>The processing status marks whether processing is complete.</td>
</tr>
<tr>
<td>Sort order</td>
<td>Order in which processing status can be set.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

You can use user-defined columns, for example, to link processing statuses to resources (Spare field no. 01 to Spare field no. 10) To use the processing status in requests,
specify **Processing status on success** and **Processing status on error** in the approval step.

**Related topics**

- Default processing status on page 168
- Editing resources on page 168
- One Identity Manager IT Shop Administration Guide

**Default processing status**

One Identity Manager provides the processing status by default. This processing status is used in IT Shop, in the approval steps of the default approval workflow.

**To display the default processing status**

1. Select Entitlements | Basic configuration data | Processing status | Predefined.

**Editing resources**

**To edit resources**

1. Select the category Entitlements | Resources.
2. Select a resource in the result list. Select Change master data.
   - OR -
   1. 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 168
- Assigning resources to employees on page 170

**Resource master data**

Enter the following master data for a resource.
### Table 71: Resource master data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Resource identifier.</td>
</tr>
<tr>
<td>Resource type</td>
<td>Resource type for grouping resources.</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item through which you can request the resource in the IT Shop. Assign an existing service item or add a new one.</td>
</tr>
<tr>
<td>Required resource</td>
<td>Define the dependencies between resources. When this resource is requested or assigned, the required resource is automatically requested or assigned with it.</td>
</tr>
<tr>
<td>Risk index</td>
<td>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 configuration parameter QER</td>
</tr>
<tr>
<td>IT Shop</td>
<td>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 of IT Shop.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>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.</td>
</tr>
<tr>
<td>No inheritance on security risk</td>
<td>Resources marked with this option are not inherited by employee who are rated as a security risk.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Automatic assignment to employees</td>
<td>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. Disable this option to remove automatic assignment of the resource to all employees. The resource cannot be reassigned to employees from this point on. Existing resource assignments remain intact.</td>
</tr>
<tr>
<td>Spare field no. 01 ... Spare field no. 10</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

**Related topics**

- Resource types on page 166
- 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 (department, cost center, location or business role).

Detailed information about this topic

- Permitting assignments of employees, devices, workdesks, and company resources on page 24
- 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 Entitlements | Resources.
2. Select a resource in the result list.
3. Select Assign organizations.
4. Assign organizations in Add assignments.
   - Assign departments on the Departments tab.
   - Assign locations on the Locations tab.
   - Assign cost centers on the Cost centers tab.

**TIP:** In the Remove assignments area, you can remove the assignment of 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 29
- Basic principles 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 category Entitlements | Resources.
2. Select a resource in the result list.
3. Select Assign business roles in the task view.
4. Assign business roles in Add assignments.
   - TIP: In the Remove assignments area, you can remove the assignment of 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 category Entitlements | Resources.
2. Select a resource in the result list.
3. Select Assign to employees in the task view.
4. Assign employees in **Add assignments**.

   **TIP:** In the **Remove assignments** area, you can remove the assignment of employees.

   **To remove an assignment**
   - Select an assignment and double-click.

5. Save the changes.

**Related topics**
- Employee administration on page 72
- 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 **Only use in IT Shop** 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 category **Entitlements | Resources**.
2. Select a resource in the result list.
3. Select **Add to IT Shop**.
4. In **Add assignments**, assign the resource to the IT Shop shelves.
5. Save the changes.

**To remove a resource from individual IT Shop shelves**
1. Select the category **Entitlements | Resources**.
2. Select a resource in the result list.
3. Select **Add to IT Shop**.
4. In **Remove assignments**, remove the resource from the IT Shop shelves.
5. Save the changes.
To remove resource from all IT Shop shelves

1. Select the category **Entitlements | Resources**.
2. Select a resource in the result list.
3. Select **Remove from all shelves (IT Shop)**.
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 168
- 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 by which "Only use in IT Shop" can only be assigned to system roles which also have the option set.

To assign a resource to system roles

1. Select the category **Entitlements | Resources**.
2. Select a resource in the result list.
3. Select **Assign system roles**.
4. Assign system roles in **Add assignments**.
   - OR -
     Delete the system roles in **Remove assignments**.
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 category Entitlements | Resources.
2. Select a resource in the result list.

Assigning extended properties to a resource

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

To specify extended properties for an resource

1. Select the category Entitlements | Resources.
2. Select a resource in the result list.
3. Select Assign extended properties in the task view.
4. Assign extended properties in Add assignments.
   - OR -
   Remove extended properties from Remove assignments.
5. Save the changes.

Detailed information about this topic

- Edit extended properties on page 181
Editing multi-request resources

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

- Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.

To edit multi-request resources
1. Select Entitlements | Multi-request resources for IT Shop.
2. Select a resource in the result list. Select Change master data.
   - 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 Entitlements | Multi-requestable/unsubscribable resources for IT Shop.
2. Select a resource in the result list. Select Change master data.
   - 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 175
- Assigning multi-request resources to employees on page 176

Master data for a multi-request resource

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

Table 72: Multi-Request Resource Master Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-request resource</td>
<td>Resource identifier.</td>
</tr>
<tr>
<td>Multi-</td>
<td></td>
</tr>
</tbody>
</table>

One Identity Manager 8.1.1 Identity Management Base Module Administration Guide Managing resources 175
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>requestable/unsubscribable resource</td>
<td></td>
</tr>
<tr>
<td>Resource type</td>
<td>Resource type for grouping resources.</td>
</tr>
<tr>
<td>Service item</td>
<td>Service item through which you can request the resource in the IT Shop. Assign an existing service item or add a new one.</td>
</tr>
<tr>
<td>Risk index</td>
<td>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 configuration parameter QER</td>
</tr>
<tr>
<td>IT Shop</td>
<td>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 of IT Shop. This option cannot be disabled.</td>
</tr>
<tr>
<td>Only for use in IT Shop</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Spare field no. 01 ... Spare field no. 10</td>
<td>Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.</td>
</tr>
</tbody>
</table>

**Related topics**

- Resource types on page 166
- 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**

- Assignments via IT Shop requests on page 17
- 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 **Entitlements | Multi-request resources for IT Shop.**
   - OR -
   Select **Entitlements | Multi requestable/unsubscribable resources for IT Shop.**
2. Select a resource in the result list.
3. Select **Add to IT Shop.**
4. In **Add assignments,** assign the resource to the IT Shop shelves.
5. Save the changes.

**To remove multi request resources from individual IT Shop shelves**

1. Select **Entitlements | Multi-request resources for IT Shop.**
   - OR -
   Select **Entitlements | Multi requestable/unsubscribable resources for IT Shop.**
2. Select a resource in the result list.
3. Select **Add to IT Shop.**
4. In **Remove assignments,** remove the resource from the IT Shop shelves.
5. Save the changes.

**To remove multi-request resources from all IT Shop shelves**

1. Select **Entitlements | Multi-request resources for IT Shop.**
   - OR -
   Select **Entitlements | Multi requestable/unsubscribable resources for IT Shop.**
2. Select a resource in the result list.
3. Select **Remove from all shelves (IT Shop)**.
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.

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

**Table 73: Reports about Resources**

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of all assignments</td>
<td>This report finds all roles containing employees with the selected resource.</td>
</tr>
</tbody>
</table>

**Related topics**
- Analyzing role memberships and employee assignments on page 121
Set up extended properties

Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas. 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 180
- Edit extended properties

One Identity Manager users for managing extended properties

The following users are used for managing extended properties.

Table 74: Users

<table>
<thead>
<tr>
<th>Users</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators for the IT Shop</td>
<td>Administrators must be assigned to the Request &amp; Fulfillment</td>
</tr>
<tr>
<td></td>
<td>Users with this application role:</td>
</tr>
<tr>
<td>Users</td>
<td>Task</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
</tr>
</tbody>
</table>
| One Identity Manager administrators | • Create extended properties for company resources of any type.  
• Create customized permissions groups for application roles for role-based login to administration tools in Designer as required.  
• Create system users and permissions groups for non-role-based login to administration tools in Designer as required.  
• Enable or disable additional configuration parameters in Designer as required.  
• Create custom processes in Designer as required.  
• Create and configures 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. Select Entitlements | Basic configuration data | Extended properties.
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. Select Entitlements | Basic configuration data | Extended properties.
2. Select a property group in the result list.
3. Select Assign extended properties.
4. Assign extended properties in Add assignments.
   - OR -
   Remove extended properties from Remove assignments.
5. Save the changes.
Edit extended properties

To edit an extended property

1. Select Entitlements | Basic configuration data | Extended properties | <property group>.
2. Select the extended property in the result list. Select Change master data.
   - 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 181
- Specifying scope boundaries on page 182

Extended property master data

Enter the following data for an extended property.

Table 75: Extended Property Master Data

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended property name</td>
<td>Name of the extended property.</td>
</tr>
<tr>
<td>Property group</td>
<td>The property group for structuring extended properties. You can assign a</td>
</tr>
<tr>
<td></td>
<td>primary property group to a property on the master data form. Extended</td>
</tr>
<tr>
<td></td>
<td>properties are grouped by this property group in navigation. If an</td>
</tr>
<tr>
<td></td>
<td>extended property needs to be assigned to several property groups, then</td>
</tr>
<tr>
<td></td>
<td>you can use the task Assign property groups to assign additional</td>
</tr>
<tr>
<td></td>
<td>property groups.</td>
</tr>
<tr>
<td>Lower scope boundary</td>
<td>Lower scope boundary for further subdivision.</td>
</tr>
<tr>
<td>Upper scope boundary</td>
<td>Upper scope boundary for further subdivision.</td>
</tr>
<tr>
<td>Description</td>
<td>Spare text box for additional explanation.</td>
</tr>
<tr>
<td>Spare field</td>
<td>Additional company specific information. Use Designer to customize</td>
</tr>
</tbody>
</table>
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. Select Entitlements | Basic configuration data | Extended properties | <property group>.
2. Select the extended property in the result list.
3. Select Extended property overview.

To obtain an overview of a property group

1. Select Entitlements | Basic configuration data | Extended properties.
2. Select a property group in the result list.
3. Select Property group overview.

Assigning objects

You can assign extended properties to company resources, hierarchical roles, and employees.

To assign objects to an extended property

1. Select Entitlements | Basic configuration data | Extended properties | <property group>.
2. Select the extended property in the result list.
3. Select Assign objects.
4. Select the desired object type in Select object type.
   The object belonging to the object types are displayed on the form.
5. Assign objects in Add assignments.
   - OR -
   Remove objects in Remove assignments.
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. Select Entitlements| Basic configuration data | Extended properties | <property group>.
2. Select the extended property in the result list.
3. Select Assign property groups.
4. Assign property groups in Add assignments.
   - OR -
   Remove property groups in Remove assignments.
5. Save the changes.

Related topics

- Create property groups on page 180
Appendix: 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 76: Configuration parameters**

<table>
<thead>
<tr>
<th>Configuration parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
</tbody>
</table>
| QER | Structures | ExcludeStructures | Preprocessor relevant configuration parameter for defining the effectiveness of role memberships. If this
<table>
<thead>
<tr>
<th>Configuration parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
<tr>
<td>QER</td>
<td>Structures</td>
</tr>
</tbody>
</table>
Appendix: Configuration parameters for managing employees

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

Table 77: Configuration parameter

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>Person</td>
<td>MasterIdentity</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
<tr>
<td>QER</td>
<td>Person</td>
</tr>
</tbody>
</table>
| QER | Person | TemporaryDeactivation | This configuration parameter controls the behavior between employees and user accounts if employees are temporarily inactivated.  
If the configuration parameter is set, the employee’s user accounts are locked if the employee is permanently or temporarily disabled.  
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 | 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. |
| 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. |</p>
<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SysConfig</td>
<td>Display</td>
</tr>
</tbody>
</table>
Appendix: 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 78: Configuration parameters

<table>
<thead>
<tr>
<th>Configuration parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Preprocessor relevant configuration parameter to control the database model components for device administration. If the parameter is set, the device administration components are available. The database must be recompiled after changes have been made to the parameter.</td>
</tr>
<tr>
<td>Hardware</td>
<td>AssetAccounting</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td><strong>Configuration parameters</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>PC</strong></td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Display</td>
</tr>
<tr>
<td>Hardware</td>
<td>Workdesk</td>
</tr>
<tr>
<td>Hardware</td>
<td>Workdesk</td>
</tr>
</tbody>
</table>
About us

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

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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
administrator identity
   personal 92
application
   assign to employees 117
   assign to workdesks 154
application role
   administrators 29, 73
   approver 36
   approver(IT) 36
   assign employees 115
attestor 29, 35
basic roles
   employee managers 73
employee managers 73
identity management
   employees
   administrators 73
Identity Management
   organizations
   administrators 29
   attestor 29
asset class 158
asset type 159
assignment
   company resources 22
   direct 14
   dynamic role 17
   indirect 14
   primary 16
   configuration 16
   secondary 15
      configuration 24
      permit 24
      via IT Shop request 17
B
base object
   mail template 77
business partner 75, 134
C
company resources
   assign 14, 52, 110, 143, 151
configuration parameter 185, 187, 190
cost center
   administrators 29
   approver 36, 42
   approver(IT) 36, 42
   assign company resources 22, 52
   assign devices 51, 144
   assign employees 51, 113
   assign workdesks 51, 113
   attestor 29, 35, 42
   basics 10
   conflicting roles 27, 61
   country 45
   dynamic 59
   edit 42
   functional area 45
   IT operating data 54
manager 42
no inheritance 26, 42
permit assignment 24
profit 45
risk index 45
rule violations 45
short name 42
specify role relations 62
state 45
transparency index 45
turnover 45

D
department
administrators 29
approver 36, 38
approver(IT) 36, 38
assign company resources 22, 52
assign devices 51, 144
assign employees 51, 113
assign workdesks 51, 152
attestor 29, 35, 38
basics 10
conflicting roles 27, 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
permit assignment 24
profit 41
risk index 41
rule violations 41
short name 38
specify role relations 62
state 41
transparency index 41
turnover 41
device
asset class 158, 160
asset data 157
asset type 159-160
assign business role 139
assign company resources 143
assign cost center 139
assign department 139
assign location 139
assign to business role 145
assign to cost center 144
assign to department 144, 160
assign to location 144
assign to workdesk 156
assign workdesk 139
company 134
device ID 139
device model 131, 139
device status 135, 160
edit 137
enter call 147
location 160
network configuration 141
no inheritance 26, 139
service agreement 147
workdesk 147
device model
device type 132
disability 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
dynamic role
calculate 69-70
condition 66
test 68
cost center 59
department 59
location 59
schedule 66
set up 66

E
employee
add to IT Shop 115
address 84
area of responsibility 122
assign application 117
assign application role 115
assign business role 83, 114
assign company resources 110
assign cost center 51, 83, 113
assign department 51, 83, 113
assign extended property 123
assign location 51, 113
assign reports 118
assign resource 116
assign system role 117
assign to workdesk 80, 156
central password 86, 89
password question 124
reset 125
central SAP user account 86
central user account 86, 88
certification status 80, 109
company 80
country 84, 126-127
default email address 86, 90
delete 96
deploy 83
dummy employee 86
employee managers 73
enter call 123
entry date 83
external 80
ID number 83
identity 86
language 84, 126
leaving date 83
limit access 108
location 84
locked 108
log 79
logins 86
main identity 86, 91
manager 83
mutual aid 124-125
new user 108
no inheritance 26, 80
permanently disable 94
permanently disabled 80
picture 84
re-enable 94-95
reactivate 95
reports 128
risk index 80
security risk 80
Starling 2FA user ID 86
state 84, 126-127
sub-identity 91
system user 86
telephone 84
temporarily deactivate 94
temporarily disable 83
user account 122-123
working hours 127
X500 employee 86
employee managers 73
extended property 179
assign objects 183
assign resources 174
assign to employees 123
create 181
extended property group 184
overview form 183
property group 181
scope boundary 181-182

I
identity
organizational 92
primary 92
inheritance
bottom-up 10
calculate 18-20
discontinue 12
limit 26
top-down 10
XIsInEffect 20
XOrigin 20
inheritance direction 10
inheritance exclusion 27
define for roles 61
IT operating data 54
change 58

L
leasing provider 134
company 75
location
address 48-49
administrators 29
approver 36, 46
approver(IT) 36, 46
assign company resources 22, 52
assign devices 51, 144
assign employees 51, 113
assign workdesks 51, 152
attester 29, 35, 46
basics 10
conflicting roles 27, 61

F
functional area 34

G
group identity 92
country 48
dynamic 59
edit 46
functional area 50
IT operating data 54
manager 46
network configuration 49
no inheritance 26, 46
permit assignment 24
profit 50
risk index 50
rule violations 50
short name 46
specify role relations 62
state 48
transparency index 50
turnover 50

M
mail definition 78
mail template
   base object 77-78
manufacturer 75, 134
mutual aid 124-125

N
notification
   mail template 76

O
overview form
   extended property 183
resource 174

P
password
   central 86, 89
      password question 124
   reset 125
password policy 96
   assign 98
   character classes 102
   check password 106
   default policy 98, 101
   display name 101
   editing 100
   error message 101
   excluded list 106
   failed logins 101
   generate password 107
   generation script 103, 105
   initial password 101
   name properties 101
   password age 101
   password cycle 101
   password length 101
   password strength 101
   predefined 97
   test script 103-104
person
   administrators 73
processing status
   default processing status 168
property group 179
   assign extended properties 184
   create 180
resource 164
  assign extended properties 174
assign system role 173
assign to employees 116, 168
inheritance 168, 175
overview form 174
requestable 168, 175
resource type 168, 175
risk index 168, 175
service item 168, 175
set up 168
resource type 168, 175
processing step 166
set up 166
risk assessment
  functional area 34
risk index
  for resource 168, 175
role
  conflicting roles 27
role classes 32
role type 34
roles
  assign company resources 22
basics 10
inheritance
  bottom-up 10
top-down 10
no inheritance 26
permit assignment 24

service ID 92
service item
  for resource 168, 175
sponsored identity 92
subscribable report
  assign to employee 118
supplier 75, 134
system role
  add resources 173
  assign to employees 117
  assign to workdesk 155
system user 86
  locked 108

template
  IT operating data, modify 58

user account
  apply template 58

workdesk
  assign applications 154
assign company resources 151
assign cost center 51, 152
assign department 51, 149, 152
assign device 156
assign employees 156
assign location 51, 149, 152
assign system roles 155
assign to business role 148, 153
assign to cost center 148
create automatically 147
edit 147
enter call 157
no inheritance 26, 148
service agreement 157
status 148
workdesk status 136
workdesk type 136, 148
workdesk status 136
workdesk type 136