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 Business Roles Administration Guide
Updated - August 2019
Version - 8.1.1
User-defined master data for a business role .............................................. 34
Assigning employees, devices and workdesks to business roles .................... 35
Assigning business roles to company resources ........................................ 35
Analyzing role memberships and employee assignments ............................ 38
Setting up IT operating data ...................................................................... 39
  Modify IT operating data ........................................................................ 42
Additional tasks for managing business roles .............................................. 43
  Creating dynamic roles .......................................................................... 43
  Assigning organizations ........................................................................ 44
  Defining inheritance exclusion for business roles ..................................... 45
  Assigning extended properties ................................................................ 46
  Creating assignment resources ............................................................... 46
Reports about business roles ...................................................................... 46

Role mining in One Identity Manager ......................................................... 48
Cluster analysis as a basis for role mining .................................................... 49
Working with the Analyzer program .......................................................... 50
  Menu items ............................................................................................ 50
  Customizing the program settings .......................................................... 50
Running an analysis .................................................................................. 51
  Selecting analysis data using the wizard ................................................. 52
  Predefined analyses ............................................................................... 54
Analysis evaluation ................................................................................... 55
Transferring changes .................................................................................. 57

About us ..................................................................................................... 59
Contacting us ............................................................................................. 59
Technical support resources ....................................................................... 59

Index .......................................................................................................... 60
Managing 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. Various company resources can be assigned to business roles, for example, authorizations in different SAP systems or applications. You can add employees to single business roles as members. Employees obtain their company resources through these assignments when the One Identity Manager is appropriately configured.

The One Identity Manager components for managing business roles are available if "QER/Org" is set.

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

One Identity Manager users for business roles

The following users are used for managing business roles.

Table 1: User

<table>
<thead>
<tr>
<th>User</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business roles admins</td>
<td>Administrators must be assigned to the application role Identity Management</td>
</tr>
<tr>
<td></td>
<td>Users with this application role:</td>
</tr>
<tr>
<td></td>
<td>- Create and edit business roles.</td>
</tr>
<tr>
<td></td>
<td>- Assign company resources to business roles.</td>
</tr>
<tr>
<td></td>
<td>- Administrate application roles for role approvers, role approvers (IT), and attestors.</td>
</tr>
<tr>
<td></td>
<td>- Set up other application roles as required.</td>
</tr>
<tr>
<td>One Identity</td>
<td>Create customized permissions groups for application roles</td>
</tr>
<tr>
<td>User</td>
<td>Task</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Manager administrators      | 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.  |
| Business Role Attestors     | Attestors must be assigned to Identity Management | Business roles | Attestors or a child application role.  
Users with this application role:  
- Attest correct assignment of company resource to business roles for which they are responsible.  
- Can view master data for these business roles but not edit them.  |

**NOTE:** This application role is available if the module Attestation Module is installed.

### Hierarchical role structure basic principles

Business 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.

### 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**

![Diagram of top-down inheritance](image)
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.

Figure 2: Assignment through Bottom-Up Inheritance

Discontinuing inheritance

There are particular cases where you may not want to have inheritance over several hierarchical levels. That is why it is possible to discontinue inheritance within a hierarchy. The point at which the inheritance should be discontinued within a hierarchy is specified by **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.
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.
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 whether a secondary assignment of company resources to employees, device, and workdesk is possible.
Figure 7: Secondary Assignment Inheritance Schema

Related topics

- Permitting assignments of employees, devices, workdesks, and company resources on page 20

Primary assignment

You make a primary assignment by referencing a business role 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 enabled through configuration parameters. Primary assignment is enabled by default for employee objects.

Figure 8: A Primary Assignment Schema
NOTE: Changes to the configuration parameter result in the inheritance data being recalculated! That means: if the primary assignment is disabled at a later date, the inheritance data created in this way will be removed from the database.

Table 2: 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>

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 business role in this way; if an employee leaves the business role they immediately lose the resources assigned to them.

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.
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.

### Table 3: BaseTree table views

<table>
<thead>
<tr>
<th>View</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORG</td>
<td>Graphical representation of business roles</td>
</tr>
</tbody>
</table>

1. **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 4: 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 business roles for company resource assignments

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.
- Define the direction of inheritance with the hierarchy.
- 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

- Permitting assignments of employees, devices, workdesks, and company resources on page 20
- Specifying the direction of inheritance on page 21
- Using business roles to limit inheritance on page 21
- Defining inheritance exclusion for business roles on page 45

Possible company resource assignments

Employees, devices and workdesks can inherit company resources though 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 5: Possible Assignments of Company Resources through Roles

<table>
<thead>
<tr>
<th>Assignable Company Resource</th>
<th>Members in Roles</th>
<th>Workdesks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>possible</td>
<td>-</td>
</tr>
<tr>
<td>Account definitions</td>
<td>possible</td>
<td></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>
<td></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>
<td>-</td>
</tr>
<tr>
<td>SharePoint groups</td>
<td>possible (assigns to all an employee's SharePoint user accounts)</td>
<td>-</td>
</tr>
<tr>
<td>SharePoint roles</td>
<td>possible (assigns to all an employee's SharePoint user accounts)</td>
<td>-</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>
<td>-</td>
</tr>
<tr>
<td>Notes groups</td>
<td>possible (assigns to all an employee's Notes user accounts)</td>
<td>-</td>
</tr>
<tr>
<td>SAP groups</td>
<td>possible (assigns to all an employee's SAP user accounts in the same SAP client.)</td>
<td></td>
</tr>
<tr>
<td>SAP profiles</td>
<td>possible (assigns to all an employee's SAP user accounts in the same SAP client.)</td>
<td></td>
</tr>
<tr>
<td>SAP roles</td>
<td>possible (assigns to all an employee's SAP user accounts in the same SAP client.)</td>
<td></td>
</tr>
<tr>
<td>Structural profiles</td>
<td>possible (assigns to all an employee's SAP user accounts in the same SAP client.)</td>
<td></td>
</tr>
<tr>
<td>BI analysis authorizations</td>
<td>possible (assigns to all an employee's BI user accounts in the same system)</td>
<td></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>
<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>
<td>-</td>
</tr>
<tr>
<td>Assignable Company Resource</td>
<td>Members in Roles</td>
<td>Workdesks</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------</td>
<td>-----------</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>
<td>-</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>
<td>-</td>
</tr>
<tr>
<td>Unix groups</td>
<td>possible (assigns to all an employee's Unix user accounts)</td>
<td>-</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>
<td>-</td>
</tr>
<tr>
<td>System roles</td>
<td>possible</td>
<td>possible</td>
</tr>
<tr>
<td>Subscribable reports</td>
<td>possible</td>
<td>-</td>
</tr>
<tr>
<td>Applications</td>
<td>possible</td>
<td>possible</td>
</tr>
</tbody>
</table>

**Related topics**

- Assigning business roles to company resources on page 35

**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.

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 business role, set Assignment allowed and Direct assignment allowed on "business role" for "employees".

If employees can only obtain membership in a business role through the IT Shop, set Assignment allowed but not Direct assignment allowed on the role class "business role" for "employees". A corresponding assignment resource must be available in the IT Shop.

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.

Specifying the direction of inheritance

The direction of inheritance decides the distribution of company resources within a role hierarchy. The direction of inheritance is defined by the role classes.

The direction of inheritance can only be specified when a role class is added.

- Set Inherited top down to specify top-down inheritance.
- Set Inherited bottom up to specify bottom-up inheritance.

Detailed information about this topic

- Inheritance directions within a hierarchy on page 6
- Role classes on page 26

Using business 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 8

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 business roles 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

The business role B has been entered as conflicting role in business role Jenna Miller and Hans Peter are members of business role A. Louise Lotte is member of business role B. Hans Peters cannot be assigned to business role B. Apart from that, One Identity Manager also prevents Jenna Miller from being assigned to business role B and Louise Lotte to business role A.
**Figure 12: Members in Conflicting Roles**

![Diagram of members in conflicting roles]

To configure inheritance exclusion

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

Related topics

- Defining inheritance exclusion for business roles on page 45

**Basic data for structuring business roles**

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 business roles 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 business roles 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 business roles 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 business roles 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 26
- Role types on page 27
- Functional areas on page 27
- Attestors on page 28
- Role approvers and role approvers (IT) on page 29
Role classes

Business roles are grouped by role class in the navigation view. Each business role is assigned to exactly one role class. You must define suitable role classes before you can add business roles.

To edit role classes

1. Select the Business roles | 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. 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>Inherited top-down</td>
<td>Direction of inheritance top-down.</td>
</tr>
<tr>
<td>Inherited bottom-up</td>
<td>Direction of inheritance bottom-up</td>
</tr>
<tr>
<td>Delegable</td>
<td>Specifies whether memberships in roles of this role class can be delegated.</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>

NOTE: This property is available if the Attestation Module is installed.
Related topics

- Inheritance directions within a hierarchy on page 6
- Permitting assignments of employees, devices, workdesks, and company resources on page 20

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 Business roles | 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 business roles. Proceed as follows:
1. Set up functional areas.
2. Assign business roles to the functional areas.
3. Define assessment criteria for the business roles.
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 **Business Roles | 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>
</tbody>
</table>
| Max. number of rule violations| List of rule violation valid for this functional area. This value can be evaluated during the rule check.  
   **NOTE:** This input field is available if the Compliance Rules Module exists. |
| Description                   | 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 business roles 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 business roles 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>
<thead>
<tr>
<th>User</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Role</td>
<td>Attestors must be assigned to Identity Management</td>
</tr>
<tr>
<td>Business Role</td>
<td>Users with this application role:</td>
</tr>
<tr>
<td>Attestors</td>
<td>• Attest correct assignment of company resource to business roles</td>
</tr>
<tr>
<td></td>
<td>for which they are responsible.</td>
</tr>
<tr>
<td></td>
<td>• Can view master data for these business roles but not edit them.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This application role is available if the module Attestation Module is installed.</td>
</tr>
</tbody>
</table>

To specify attestors

1. Select Business roles | Basic configuration data | Attestors.
2. Select Assign employees.
3. Assign employees in Add assignments.

   **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.

Role approvers and role approvers (IT)

In One Identity Manager, you can assign business roles 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 business roles 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>
| Business Role Approvers | Approvers must be assigned to the application role Identity Management | Business roles | Role approvers or a child application role. Users with this application role:  
* Are approvers for the IT Shop.  
* Approve requests from business roles for which they are responsible. |
| Business Role Approvers (IT) | IT role approvers must be assigned to Identity Management | Business roles | Role approvers (IT) or a child application role. Users with this application role:  
* Are IT role approvers for the IT Shop.  
* Approve requests from business roles for which they are responsible. |

To specify a role approver or role approver (IT)

1. Select Business roles | Basic configuration data | Approver.  
   - OR -  
   Select Business roles | 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.

Editing business roles

Business roles are grouped by role class in the navigation view. Each business role is assigned to exactly one role class. You must define suitable role classes before you can add business roles. For more information, see Role classes on page 26.
**To edit business roles**

1. Select the category **Business roles | <Role class>**.
2. Select a business role in the result list. Select **Change master data**.
   - OR -
   Click 🖼 in the result list.
3. Edit the business role's master data.
4. Save the changes.

**General master data for a business role**

Enter the following master data for a business role.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business role</td>
<td>Business role name.</td>
</tr>
<tr>
<td>Short name</td>
<td>Short name for the business role.</td>
</tr>
<tr>
<td>Internal name</td>
<td>Additional identifier for the business role.</td>
</tr>
<tr>
<td>Role classes</td>
<td>Role class to which the business role is assigned. The value is preset with</td>
</tr>
<tr>
<td></td>
<td>the role classes selected in the navigation view. If a new business role is</td>
</tr>
<tr>
<td></td>
<td>added, you can assign any role class to it.</td>
</tr>
<tr>
<td>Parent business role</td>
<td>Parent of business role in the hierarchy.</td>
</tr>
<tr>
<td></td>
<td>To organize business roles hierarchically, select the parent business role in</td>
</tr>
<tr>
<td></td>
<td>the menu. Only the business roles that belong to the same role class can be</td>
</tr>
<tr>
<td></td>
<td>selected. Leave this field empty if the business role is at the top level of</td>
</tr>
<tr>
<td></td>
<td>the business role hierarchy.</td>
</tr>
<tr>
<td>Role type</td>
<td>Select a role type from the menu.</td>
</tr>
<tr>
<td></td>
<td>To create a new role type, click 🖼. Enter a name and description for the</td>
</tr>
<tr>
<td></td>
<td>role type.</td>
</tr>
<tr>
<td>Role approver</td>
<td>Application role whose members approve IT Shop requests for members of this</td>
</tr>
<tr>
<td></td>
<td>business role.</td>
</tr>
<tr>
<td></td>
<td>To create a new application role, click 🖼. Enter the application role name</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>business role.</td>
</tr>
<tr>
<td></td>
<td>To create a new application role, click 🖼. Enter the application role name</td>
</tr>
</tbody>
</table>
### Property | Description
--- | ---
Manager | Manager responsible for the business role.
Deputy manager | Deputy business role manager.
Attestors | Applications role whose members are authorized to approve attestation cases for this business role.

To create a new application role, click ![add icon](add_icon). Enter the application role name and assign a parent application role.

**NOTE:** This property is available if the Attestation Module is installed.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Department to which the business role is primary assigned.</td>
</tr>
<tr>
<td>Location</td>
<td>Location to which the business role is primary assigned.</td>
</tr>
<tr>
<td>Cost center</td>
<td>Cost center to which the business role is primary assigned.</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>Business role certification status. You can select the following certification statuses:</td>
</tr>
<tr>
<td></td>
<td>l New - The business role has been added to the One Identity Manager database.</td>
</tr>
<tr>
<td></td>
<td>l Certified - The business role's master data has been granted approval by a manager.</td>
</tr>
<tr>
<td></td>
<td>l Denied - The business role's master data has been denied approval by a 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>Block inheritance</td>
<td>Specifies whether inheritance for this business role can be discontinued. Set this option to discontinue inheritance within the business role 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 business role.</td>
</tr>
<tr>
<td>Devices do not inherit</td>
<td>Specifies whether device inheritance should be temporarily prevented for this business role.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workdesks do not inherit</td>
<td>Specifies whether workdesk inheritance should be temporarily prevented for this business role.</td>
</tr>
<tr>
<td>Dynamic roles not allowed</td>
<td>Specifies whether a dynamic role can be created for the business role.</td>
</tr>
</tbody>
</table>

**Related topics**

- Role classes on page 26
- Role types on page 27
- Role approvers and role approvers (IT) on page 29
- Attestors on page 28
- Using business roles to limit inheritance on page 21
- Creating dynamic roles on page 43

### Business role address data

Enter the following master data for contacting the business role.

**Table 12: Business role address data**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Business role mail address</td>
</tr>
<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>Country</td>
<td>Country. You require this to determine the employee’s language and working hours. For more information, see the One Identity Manager Identity Management Base Module Administration Guide.</td>
</tr>
<tr>
<td>State</td>
<td>State. You require this to determine the employee’s language and working hours. For more information, see the One Identity Manager Identity Management Base Module Administration Guide.</td>
</tr>
<tr>
<td>Phone</td>
<td>Business role telephone number.</td>
</tr>
<tr>
<td>Quick dial</td>
<td>Telephone short entry (without code).</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room</td>
<td>Room.</td>
</tr>
<tr>
<td>Comment (room)</td>
<td>Spare text box for additional explanation.</td>
</tr>
</tbody>
</table>

## Functional area and risk assessment

Here, you can enter values to classify the business roles, which analyze the risk of a business role with respect to identity audit.

### Table 13: Master data of a business role's functional area

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional area</td>
<td>Department functional area This data is required for department's risk assessment. For more information, see Functional areas on page 27.</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\CalculateRiskIndex&quot; configuration parameter is set. For detailed information, see the One Identity Manager Risk Assessment Administration Guide.</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.</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 department. The value can be evaluated when compliance rules are checked.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This property is only available if the Compliance Rules Module is installed.</td>
</tr>
<tr>
<td>Turnover for this unit</td>
<td>Business roles turnover.</td>
</tr>
<tr>
<td>Earnings for this unit</td>
<td>Business roles earnings.</td>
</tr>
</tbody>
</table>

## User-defined master data for a business role

Additional company specific information. Use Designer to customize display names, formats and templates for the input fields.
Assigning employees, devices and workdesks to business roles

In order for employees, devices, and workdesks to inherit company resources, you must assign the objects to roles.

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

1. Select the category Business roles | <Role class>.
2. Select the business 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.

TIP: Use dynamic roles to assign employees, devices, and workdesks to business roles automatically.

Related topics

- Permitting assignments of employees, devices, workdesks, and company resources on page 20
- Assigning business roles to company resources on page 35
- Creating dynamic roles on page 43

Assigning business roles to company resources

The default method of assigning employees, devices and workdesks is indirect assignment. This allocates an employee, a device or a workdesk to business roles. 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 business role 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 business roles 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 14: 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>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>
</tbody>
</table>
### Company Resource | Available in Module
--- | ---
E-Business Suite permissions | Oracle E-Business Suite Module
System roles | System Roles Module
Subscribable reports | Report Subscription Module
Applications | Application Management Module
Azure Active Directory groups | Azure Active Directory Module
Azure Active Directory administrator roles | Azure Active Directory Module
Azure Active Directory subscriptions | Azure Active Directory Module
Disabled Azure Active Directory service plans | Azure Active Directory Module
Unix groups | Unix Based Target Systems Module
Cloud groups | Cloud Systems Management Module
PAM user groups | Privileged Account Governance Module
G Suite groups | G Suite Module
G Suite products and SKUs | G Suite Module

**To add company resources to a hierarchical role**

1. Select the category **Business roles | <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 10
- [Permitting assignments of employees, devices, workdesks, and company resources](#) on page 20

**Related topics**

- [Possible company resource assignments](#) on page 18
- [Assigning employees, devices and workdesks to business roles](#) on page 35
- [Creating dynamic roles](#) on page 43
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.

Figure 13: Toolbar of the Overview of all assignments report.
### Table 15: Meaning of Icons in the Report Toolbar

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

### 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 business roles, departments, locations or cost centers. An employee is assigned a primary business role, 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 **Business roles | <role class>**.
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 16: 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. 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 <strong>Table</strong>, 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 <strong>Effects on</strong>.</td>
</tr>
<tr>
<td></td>
<td>d. Click <strong>OK</strong>.</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>
</tbody>
</table>

| Value       | Concrete value which is assigned to the user account property.               |

5. Save the changes.

The IT operating data necessary in the One Identity Manager default configuration for automatically creating or changing employee user accounts and mailboxes in the target system is itemized in the following table.

---

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

**Table 17: 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>Target system type</td>
<td>IT operating data</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------</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>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>Target system type</td>
<td>IT operating data</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------</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>

**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 role, or a location was changed.
  - OR -
- The default values in the IT operating data template were modified for an account definition.

ℹ️ **NOTE:** If the assignment of an employee to a primary business role 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 business roles

After you have entered the master data, you can run the following tasks. You can find the most important information on the overview form.

Creating dynamic roles

Use this task to define dynamic roles for individual business 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 business role in this way; if an employee leaves the department they immediately lose the resources assigned to them.

Dynamic roles always relate to the secondary role assignment of an employee object. Therefore secondary assignment of employees, devices and workdesks to role classes must be permitted. If necessary, further configuration settings need to be made. For more
information, see Permitting assignments of employees, devices, workdesks, and company resources on page 20.

NOTE: Create dynamic role is only available for business roles that do not have Dynamic roles not allowed set.

To create a dynamic role

1. Select the category Business roles | <Role class>.
2. Select a business 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 Business roles | <Role class> | Dynamic roles.
2. Select a business role in the result list.
3. Open the business 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.

For more detailed information about creating and editing dynamic roles, see the One Identity Manager Identity Management Base Module Administration Guide.

Related topics

- General master data for a business role on page 31

Assigning organizations

Use this task to map which relations exist between business roles and departments, cost centers and locations. This task has the same effect as assigning a department, cost center, or location on the business role master data form. The assignment is entered in the respective foreign key column in the base table.

To assign a department, cost center, or location to business roles

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

5. Save the changes.

### Defining inheritance exclusion for business 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 business roles 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 business role**

1. Select **Business roles | <Role class>** in Manager.
2. Select a business role in the result list.
3. Select **Edit conflicting business roles**.
4. In **Add assignments**, assign the business roles that are mutually exclusive to the selected business role.
   - OR -
   In **Remove assignments**, remove the business roles that are no longer mutually exclusive.
5. Save the changes.

### Detailed information about this topic

- **Inheritance exclusion: Specifying conflicting roles** on page 23
Assigning extended properties

You can assign extended properties to business roles. Extended properties are meta objects that cannot be mapped directly in One Identity Manager, for example, operating codes, cost codes or cost accounting areas. For more information, see the One Identity Manager Identity Management Base Module Administration Guide.

To specify extended properties for a business role

1. Select the category Business roles | <Role class>.
2. Select the business role 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.

Creating assignment resources

You may add assignment resources to single business roles. This means you can limit assignment resources to a certain business role in the Web Portal. When the assignment resource is requested, it is no longer necessary to request the business role as well. It is automatically a part of the assignment request. For more information, see the One Identity Manager IT Shop Administration Guide.

To limit an assignment resource to a business role

1. Select the category Business roles | <Role class>.
2. Select a business role in the result list.
3. Select Create assignment resource... in the task view.
   This starts a wizard, which takes you through adding an assignment resource.

Reports about business roles

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 business roles.

NOTE: Other sections may be available depending on the which modules are installed.
Table 18: Reports about Business Roles

<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 business roles are also members.</td>
</tr>
<tr>
<td>Show historical memberships</td>
<td>This report lists all members of the selected business role and the length of their membership.</td>
</tr>
<tr>
<td>Show products still to be approved</td>
<td>The report shows all products for a business role whose requests can be approved by the business role's members.</td>
</tr>
<tr>
<td>Business roles with high risk level</td>
<td>The report lists all business roles with a risk index equal or higher that the configurable risk index. The result can be limited to a specified role class. You can find this report in My One Identity Manager.</td>
</tr>
</tbody>
</table>

Related topics

- Analyzing role memberships and employee assignments on page 38
Role mining in One Identity Manager

Business roles can be formed in two ways:

- Role modelling as described in Managing business roles on page 5.
- Role mining, by analyzing existing access permissions.

One Identity Manager uses the program "Analyzer" to make its own tools available for analyzing user accounts and permissions. The Analyzer supports analysis of business roles as well as the analysis of data quality with respect to the question: how well suited is the permissions data to partially automated role mining?

The Analyzer offers:

- Automatic analysis of permissions assignments base on cluster analysis algorithms with different weighting.
- Automatic analysis of existing structures and permissions of employees assigned in them
- Manual analysis of certain staff groups for role mining

The aim of role mining is to replace direct permissions, which previously were only granted to users in individual application systems, with indirect ones. This allows permissions, which users obtain through role association to be defined across the application system.

Analyzer’s aim is not only pure role mining but also classification of roles in a simple to administer hierarchical system. This can reduce the administration workload further and increase security for granting permissions.

To user role mining in One Identity Manager

- Set "QER\Org\RoleMining" in the Designer.

**NOTE:** To use Analyzer for analyzing permissions, at least the Target System Base Module must be installed.
Cluster analysis as a basis for role mining

The basis for role mining is always a cluster analysis when Analyzer with help of mathematical algorithm tries to find single clusters, meaning employees with similar permissions. In the process, either hierarchical structures are built or predefined structures are applied that can be used for constructing your own role model.

In role mining, you not only try to find single clusters and assign these to business roles, but you also try to develop direct hierarchical role structures that can then be effectively used through standard inheritance mechanisms.

Automatic role mining supports One Identity Manager through two different cluster analysis methods that differ in the way they calculate the distances between individual clusters. The use of existing role structures, for example, organizational structure from ERP systems, is possible. With the help of permissions analysis, these can be assigned to access rights. Lastly, role structures can be freely defined and assignment of permissions and employees can be manually evaluated based on existing permissions.

Figure 14: Cluster Analysis Methods in Analyzer

In clustering methods, Analyzer calculates a frequency distribution from user permissions in the different application systems, like Active Directory, IBM Notes or SAP R/3. Certain permissions may have a higher weighting in comparison to others. The number of a permissions' members can, for example, represent this sort of criteria. This is acknowledged through the Analyzer during calculation and taken into account by weighting the distance between clusters. This allows the hierarchical structures arising from the
analysis to be optimized in advance and the smallest possible number of roles to be attained.

**Working with the Analyzer program**

Use the Analyzer to automatically detect and analyze data correlations in the database. This information can be used to replace, for example, direct permissions assignments with indirect assignments, therefore reducing the administration effort.

**Menu items**

<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu item</th>
<th>Meaning</th>
<th>Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>New connection...</td>
<td>Creates a new database connection.</td>
<td>Ctrl + Shift + N</td>
</tr>
<tr>
<td></td>
<td>Save to database...</td>
<td>Changes to the data are saved to the connected One Identity Manager database.</td>
<td>Ctrl + Shift + S</td>
</tr>
<tr>
<td></td>
<td>Settings...</td>
<td>For configuring general program settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exit</td>
<td>Exits the program.</td>
<td>Alt + F4</td>
</tr>
<tr>
<td>Analysis</td>
<td>Previous</td>
<td>Jumps to previous employee/permissions assignment.</td>
<td>Ctrl + U</td>
</tr>
<tr>
<td></td>
<td>Next assignment</td>
<td>Jumps to next employee/permissions assignment</td>
<td>Ctrl + D</td>
</tr>
<tr>
<td></td>
<td>Parent cluster</td>
<td>Swaps to parent cluster in the hierarchy.</td>
<td>Ctrl + P</td>
</tr>
<tr>
<td></td>
<td>Reanalyze</td>
<td>Reruns the analysis.</td>
<td>F9</td>
</tr>
<tr>
<td>Help</td>
<td>Analyzer help</td>
<td>Open the help program.</td>
<td>F1</td>
</tr>
<tr>
<td></td>
<td>Info...</td>
<td>Shows the version information for program.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 19: Meaning of Items in the Menu Bar**

**Customizing the program settings**

*To change the program settings*

- Select **Database | Settings**... from the menu.
### Table 20: Program settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically close analysis information</td>
<td>If this option is set and analyses are predefined, the information window is closed after analysis. If the option is not set, the information window is shown. Close the window using the Finished button.</td>
</tr>
<tr>
<td>window on completion</td>
<td></td>
</tr>
<tr>
<td>Show permissions weighting</td>
<td>Set this option to also display a weighting for the permissions.</td>
</tr>
<tr>
<td>Role naming template</td>
<td>Define a template for role names. This is used when to format new role names in predefined analysis methods. The template support following variables:</td>
</tr>
<tr>
<td>%sequence%</td>
<td>Sequential number</td>
</tr>
<tr>
<td>%object%</td>
<td>Name of first object in cluster</td>
</tr>
<tr>
<td>%property%</td>
<td>Name of first property in cluster</td>
</tr>
</tbody>
</table>

### Running an analysis

**To start analyzing with the Analyzer**

- Select **Start | One Identity | One Identity Manager | Analyzer**
- Enter the database connection data and the system ID and log onto the program.
- Select an analysis method.

### Table 21: Analysis method

<table>
<thead>
<tr>
<th>Analysis method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selecting analysis data using the wizard</td>
<td>The initial data is collected by means of a wizard. For more information, see <a href="#">Selecting analysis data using the wizard</a> on page 52.</td>
</tr>
<tr>
<td>Employee Active Directory permissions</td>
<td>The permissions of all employees with Active Directory group memberships are analyzed. For more information, see <a href="#">Predefined analyses</a> on page 54.</td>
</tr>
</tbody>
</table>

**NOTE:** The analysis method is available if the Active Directory Module is present.
<table>
<thead>
<tr>
<th>Analysis method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Active Directory permissions and departments</td>
<td>The permissions of all employees with Active Directory group memberships are analyzed. Departments with Active Directory groups are also included in the analysis. For more information, see Predefined analyses on page 54.</td>
</tr>
</tbody>
</table>

NOTE: The analysis method is available if the Active Directory Module is present.

- Verify the analysis results. For more information, see Analysis evaluation on page 55.
- Create new business roles if required and assign the employees. Add the suggested changes to the One Identity Manager database. For more information, see Transferring changes on page 57.

## Selecting analysis data using the wizard

Before you start the analysis, you collect your initial data. The Analyzer accesses all permissions information in its own database and creates a mapping table with employees and their permissions. The result can be suggestions for single roles from analyzing a single application but also cross-system roles from analyzing permissions in several systems.

**To select initial data**

1. On the Analyzer’s start page, choose Select data with wizard.
2. Click Start.
3. Specify an employee group to analyze. Select one of the following selection methods.
   - Structures
     Employees can be selected through the organization and business roles contained in One Identity Manager.
     a. Select Structures.
     b. Click Next.
     c. In the Structures list, select the organization or business role for analysis.

     The employees assigned to this structure are displayed in the Employees list. Use the Show directly/indirectly assigned employees buttons in the title bar to filter the employees.
Table 22: Icons for filtering the employee list

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![icon]</td>
<td>Show indirectly assigned employees</td>
</tr>
<tr>
<td>![icon]</td>
<td>Show directly assigned employees</td>
</tr>
<tr>
<td>![icon]</td>
<td>Show employees from child nodes</td>
</tr>
</tbody>
</table>

d. Click **Next**.

- **Query wizard**
  Define the condition used to find the employees in the database. The wizard helps you to formulate a condition (where clause) for database queries. The complete database query is composed internally. The database query references the "Person" table. For more information about using the wizard, see One Identity Manager User Guide for One Identity Manager Tools User Interface.

- **Menu**
  The list displays all the employees in the One Identity Manager database. Use **Shift + select** or **Ctrl + select** to select several employees for analysis.

- **Load wizard template**
  Load an existing configuration. Select the template file and click **Open**.

4. Click **Next**.

5. Select the target system whose user accounts and permissions will be included in the analysis. Use **Ctrl + select** to multi-select target systems.

6. Click **Next**.

7. Specify the analysis methods. The following methods are available.

Table 23: Analysis method

<table>
<thead>
<tr>
<th>Analysis method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple cluster analysis/Complex cluster analysis</td>
<td>Permissions are grouped into new business roles using cluster analysis methods and employees are assigned. The Analyzer supports automatic role mining by two different cluster analysis methods, which differ in terms of how they calculate the distances between individual clusters.</td>
</tr>
<tr>
<td>Decision hierarchy</td>
<td>Permissions are grouped into new business roles in a decision hierarchy and the employees are assigned. The number of group members is taken as the decision criteria.</td>
</tr>
<tr>
<td>Analysis method</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Structure assignment</td>
<td>The permissions are assigned to an existing structure hierarchy. The use of existing structures, for example, organizational structure from ERP systems, is possible.</td>
</tr>
<tr>
<td>Permissions analysis</td>
<td>Employee permissions are analyzed with the help of permissions analysis. Business roles are freely defined and assignments of permissions and employees are evaluated manually based on the existing permissions.</td>
</tr>
</tbody>
</table>

8. Click **Next**.

9. (Optional) To reuse the configuration at a later time, set **Save configuration as template**. Select the directory path for saving the file using the file browser and click **Save**.

10. Click **Finish** to start the analysis.

   This loads the data and starts the analysis. The results of the analysis are subsequently displayed. For more information, see **Analysis evaluation** on page 55.

11. Create a new business role if required and assign the employees. Add the suggested changes to the One Identity Manager database. For more information, see **Transferring changes** on page 57.

### Predefined analyses

**NOTE:** Analysis methods are made available when the Active Directory Module is present.

The following predefined analyses are provided:

- Employee Active Directory permissions
  The permissions of all employees with Active Directory group memberships are analyzed.

- Employee Active Directory permissions and departments
  The permissions of all employees with Active Directory group memberships are analyzed. Departments with Active Directory groups are also included in the analysis.

**To start predefined analysis**

1. Select **Active Directory employee permissions** or **Active Directory employee permissions and departments** on the Analyzer home tab.

2. Click **Start**.

   This loads the analysis data and starts analysis immediately. This may take some time, depending on the amount of data.
Analysis data is displayed depending on the program settings. Click **Expand**... to see detailed information. Click **Finish** to close the dialog box. The results of the analysis are subsequently displayed. For more information, see Analysis evaluation on page 55.

### Analysis evaluation

You should always compare the business roles with the custom structures in the case of role mining, because the mathematical methods of cluster analysis only forecast a trend. Apart from renaming nodes, you can also edit employee assignments and business role permissions directly. You can create new business roles with the Analyzer and assign them directly to employees. This makes adding and moving employees into a certain business role very simple.

View the results of the analysis in a window with various panes in the Analyzer.

#### Figure 15: Presentation of Analysis Results

- **Select applications system**
  - Load permissions
  - Load HR/structure data

- **Search for similarities**
  - In permissions
  - In business roles and organizations

- **Assign permissions to mapped role**

- **Identify clusters and collections of roles**

On the left, the clusters found by the analysis are displayed hierarchically on a tab. The nodes mapped here are named though the first employee found when analysis data is selected with wizards. The naming of predefined analysis methods follows specified rules in the program settings. You can change names using **F2** or **Rename** in the context menu.

The number of occurrences is displayed graphically in the columns `<Employees>` and `<Permissions>`. The display is normed in both columns, which means the group with the highest number of employees or permissions assigned to it corresponds to 100 percent and is represented with maximized bars.
### Table 24: Meaning of items in the context menu in view 1

<table>
<thead>
<tr>
<th>Context Menu Item</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert</td>
<td>Marks the business role for transfer into the database.</td>
</tr>
<tr>
<td>Add recursively</td>
<td>Marks the business role and its child roles for transfer into the database.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the business role from the data transfer set.</td>
</tr>
<tr>
<td>Create</td>
<td>Defines a new business role.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the business role.</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the business role.</td>
</tr>
<tr>
<td>Generate business roles names</td>
<td>Generates business role names according to the rules specified (menu &lt;Database&gt;&lt;Settings...&gt;).</td>
</tr>
<tr>
<td>Optimize business roles</td>
<td>Optimizes the business roles. Empty business roles are deleted.</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays other properties of the business role such as user accounts and permissions.</td>
</tr>
</tbody>
</table>

When a structure node is selected the employees (above) and permissions (below) contained in it are listed in view (2). You can use the color similarity bar to help identify where permissions overlap with each other and how far the user’s actual permissions situation fits to the permissions assignment of the selected role. Matching group memberships are green, but non-matching, additional group memberships are red. Directly below this, you see each of the employee’s permissions for the analyzed target systems separately. A permissions weighting is displayed depending on the program settings.

### Table 25: Meaning of items in the context menu in view 2

<table>
<thead>
<tr>
<th>Context Menu Item</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to business role</td>
<td>Adds employee/permissions to the hierarchy of the selected business role.</td>
</tr>
<tr>
<td>Remove from business role</td>
<td>Removes employee/permissions from the hierarchy of the selected business role.</td>
</tr>
<tr>
<td>Compare</td>
<td>Compares employees with each other. The result is displayed in view 3.</td>
</tr>
<tr>
<td>Mark assignments</td>
<td>Marks employee/permissions assignments in the hierarchy.</td>
</tr>
<tr>
<td>Properties</td>
<td>Shows other properties of active objects.</td>
</tr>
</tbody>
</table>

You can analyze permissions memberships of individual employees by multi-selecting in the list of employees and running a direct comparison.
To compare employee memberships

- Select employees in view (2) using Ctrl + select or Shift + select.
- Click Compare in the context menu to start comparing.

TIP: When you click on an employee in this list, they become the reference employee. The colored similarity bars are aligned to this employee.

Transferring changes

You can use the Analyzer to create new business roles and assign employees directly to them or move employees and permissions into specific business roles.

To transfer changes to the One Identity Manager database

1. Mark the business roles you want to transfer, in the hierarchy.
   Use the Insert and Recursive context menu items to do this. You can delete individual business roles from the data transfer using the Remove context menu item.
2. Select Database | Save to database... from menu to start the data transfer wizard and click Next to continue.
3. In the wizard, select the role class under which the business roles will be created in the One Identity Manager database.
   Click the button next to the menu to create a new role class.
4. Select the save options.

**Table 26: Save options for data transfer**

<table>
<thead>
<tr>
<th>Save option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete existing objects in role class</td>
<td>This option deletes existing objects in the selected role class from the One Identity Manager database.</td>
</tr>
<tr>
<td>Business roles do not inherit</td>
<td>This option disables inheritance of assignments by business roles.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Once you have checked the assignments, remove <strong>Employees do not inherit</strong> from the business roles. Use the program &quot;Manager&quot; to do this.</td>
</tr>
<tr>
<td>Delete direct assignments</td>
<td>This option removes direct permissions assignments to the employees’ user accounts.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUTION:</strong> Only set this option if you have ensured that the permissions are inherited by the employees through business roles. Otherwise this option results in a loss of permissions.</td>
</tr>
<tr>
<td>Attest new roles</td>
<td>New business roles must go through an attestation case.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This function is only available if the Attestation Module is installed.</td>
</tr>
</tbody>
</table>

5. Click **Finished** to save the data.
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
Analyzer 50
   analysis data 52
   analysis result 55
   predefined analyses 54
   program settings 50
   save changes 57
   wizard 52
application role
   approver 29
   approver (IT) 29
   attester 28
assignment
   company resources 18
   direct 10
   dynamic role 13
   indirect 11
   IT Shop 13
   permit 20
   primary 12
      configuration 12
   secondary 11
   via IT Shop request 13
assignment resource
   for a business role 46

B
business role
   assign 10
   assign company resources 18
   assign extended property 46
   attester 30
   conflicting roles 23
   delegate membership 31
   license node 30
   prevent inheritance 21
   reports 46
   set up 30
   business role structure 30

C
company resources
   assign 10
   conflicting business role 45

D
delegation 31

F
functional area 27

I
inheritance
   bottom-up 6
   discontinue 8
   top-down 6
   inheritance direction 21
   inheritance exclusion 23
   define for business roles 45
IT operating data
  change 42

R
  risk assessment
    functional area 27
  role class 26
    delegation 31
    inheritance direction 21
    permit assignment 20
  role mining 48
    analysis data 52
    analysis result 55
    Analyzer 50
    cluster analysis 49
  role type 27
  roles
    basic principles 6
    inheritance
      bottom-up 6
      top-down 6

T
  template
    IT operating data, modify 42

U
  user account
    apply template 42