One Identity Manager 8.0

Business Roles Administration Guide

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.

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

One Identity Manager Business Roles Administration Guide
Updated - October 2017
Version - 8.0

Contents

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 the configuration parameter "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

User	Task
Business roles administrators	Administrators must be assigned to the application role **Identity Management | Business roles | Administrators**. Users with this application role: • Create and edit business roles. • Assign company resources to business roles. • Administrate application roles for role approvers, role approvers (IT) and attestors. • Set up other application roles as required.
One Identity	• Create customized permissions groups for application roles for

User	Task
Manager administrators	role-based login to administration tools in the Designer, as required. • Create system users and permissions groups for non-role based login to administration tools, as required. • Enable or disable additional configuration parameters in the Designer, as required. • Create custom processes in the Designer, as required. • Create and configures schedules, as required. • Create and configure password policies, as required.
Business Role Attestors	Attestors must be assigned to the application role **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 Basics

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 the 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.

Direction of Inheritance within a Hierarchy

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

- Top-down inheritance

  The default structure within a company is realized through top-down inheritance in One Identity Manager. With its help, a company's multilevel form can be represented with main departments and respective subdepartments.

- Bottom-up inheritance

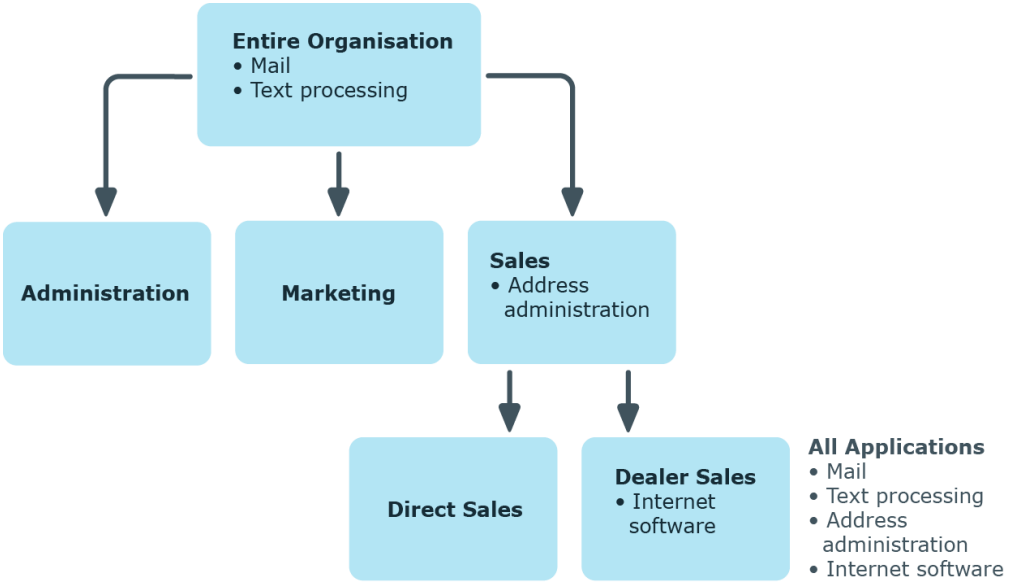
  Where as in "top-down" inheritance assignments are inherited in the direction of more detailed classifications, "bottom-up" inheritance operates in the other direction. This inheritance direction was introduced to map project groups in particular. The aim being, to provide someone coordinating several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

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

Example for Assigning Company Resources Top-Down

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

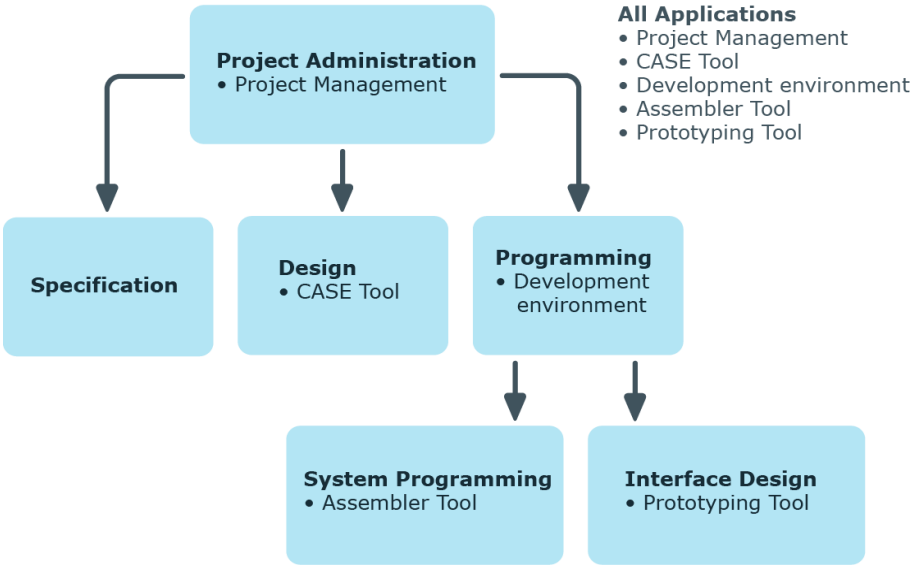
Figure 1: Assignment through Top-Down Inheritance



Example for Assigning Company Resources Bottom-Up

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

Figure 2: Assignment through Bottom-Up Inheritance



Discontinuing Inheritance

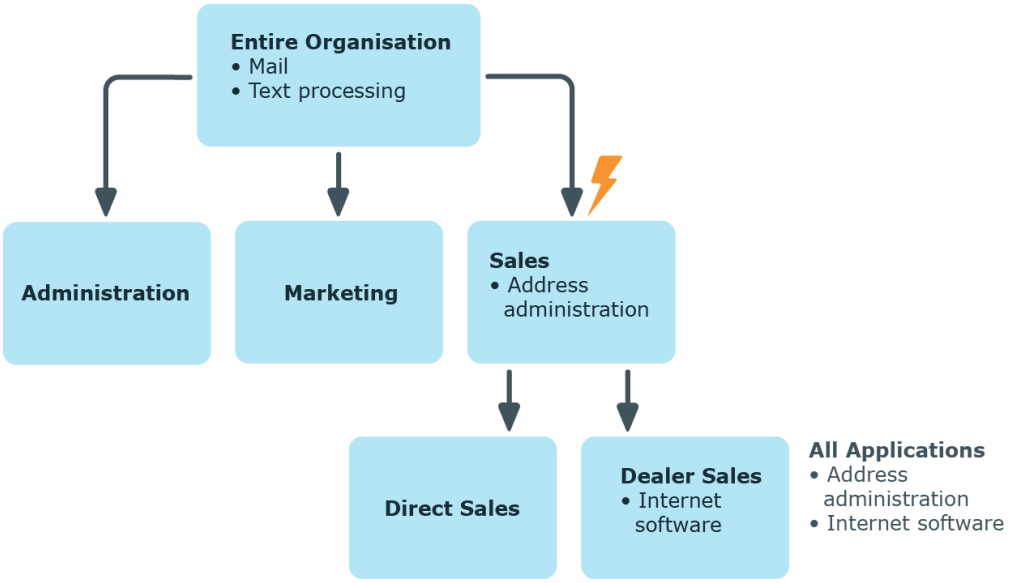
There are particular cases where you may not want to have inheritance over several hierarchical levels. That is why it is possible to discontinue inheritance within a hierarchy. The point at which the inheritance should be discontinued within a hierarchy is specified by the option **Block inheritance**.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

- Roles marked with the option **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.

Example for Discontinuing Inheritance Top-Down

If the option **Block inheritance** is set for the department "Sales" in the top-down example, it results in sales employees being assigned address administration and employees in the retail department, address administration and internet software, but neither is assigned mail or text editing applications. Applications in the department "Overall organization" are, however, not assigned to retail and dealers.

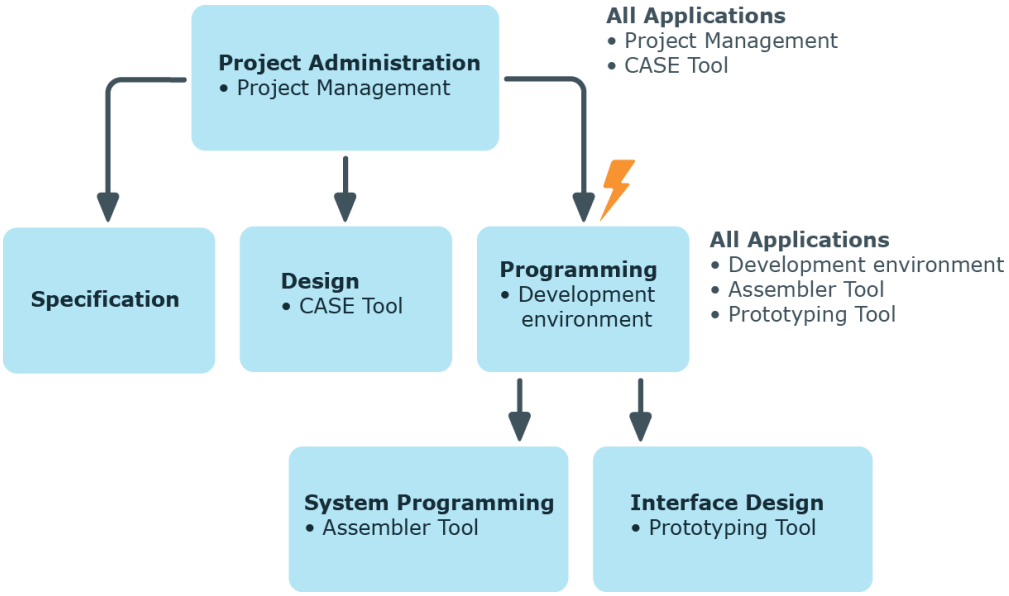
Figure 3: Discontinuing Inheritance Top-Down



Example for Discontinuing Inheritance Bottom-Up

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

Figure 4: Discontinuing Inheritance Bottom-Up



Basics 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
- Assigning through Dynamic Roles
- Assigning through IT Shop Requests

Direct Assignment

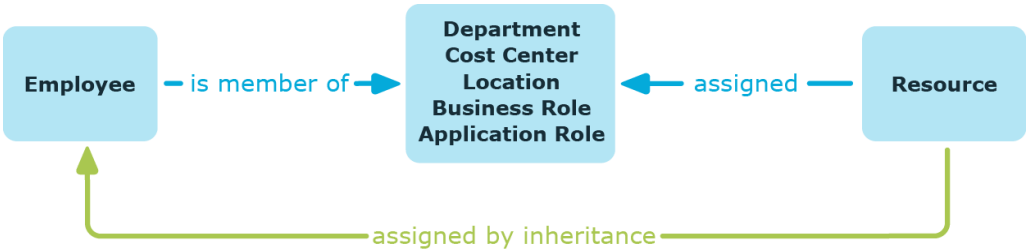
Direct assignment of company resources results from the assignment of a company resource to an employee, device or a workdesk, for example. Direct assignment of company resources makes it easier to react to special requirements.

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

Indirect Assignment

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

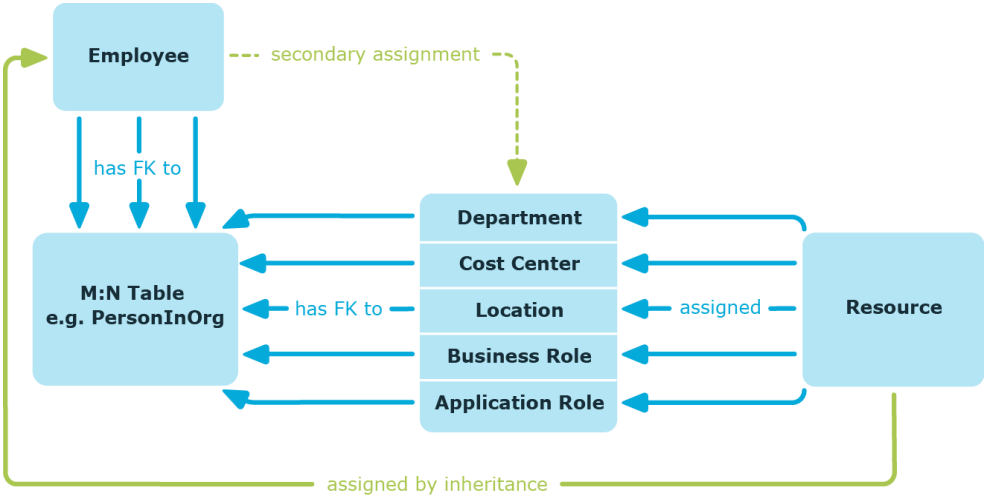
Figure 6: Schema of an indirect assignment based on the employee example



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

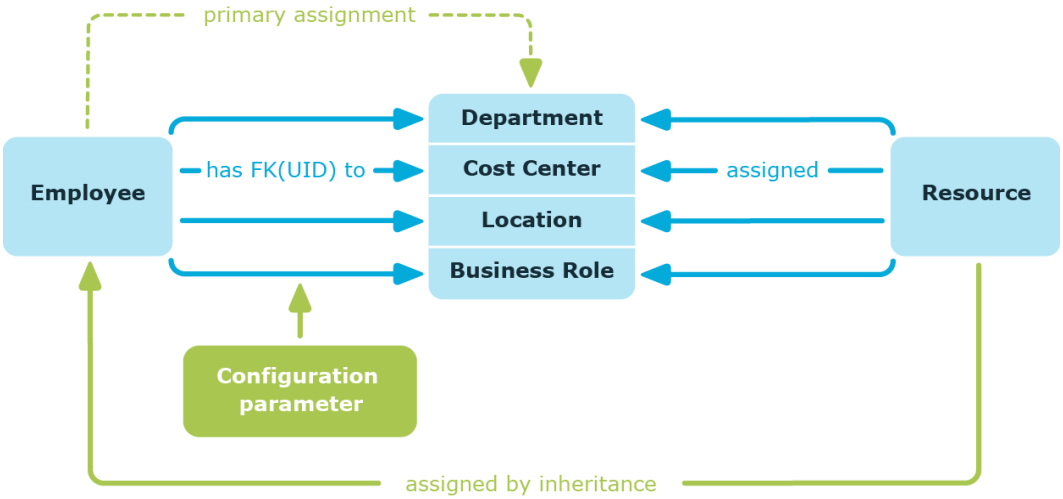
- Permit Assignments of Employees, Devices, Workdesks and Company Resources on page 19

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 enable 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

Configuration Parameter	Active Meaning
QER\Structures\Inherite\Person	Employees can inherit through primary assignments.
QER\Structures\Inherite\Person\FromOrg	Employees inherit assignments from their primary business role (Person.UID_Org).
QER\Structures\Inherite\Hardware	Devices can inherit through primary assignments.
QER\Structures\Inherite\Hardware\FromOrg	Devices inherit assignments from their primary business role (Hardware.UID_Org).
QER\Structures\Inherite\Workdesk	Workdesks can inherit though primary assignment.
QER\Structures\Inherite\Workdesk\FromOrg	Workdesks inherit assignments from their primary business role (Workdesk.UID_Org).

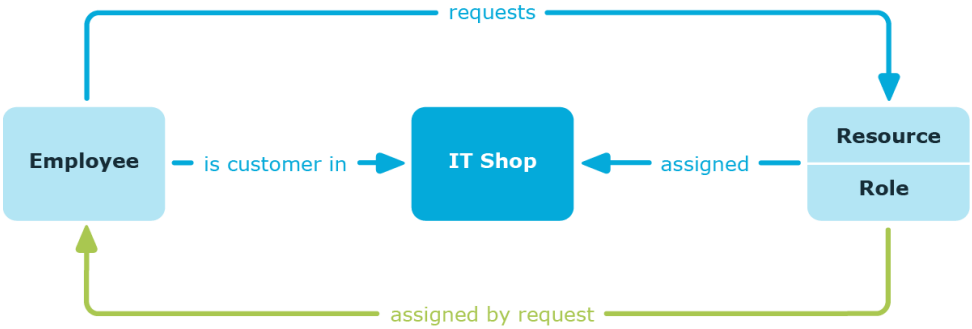
Assigning through Dynamic Roles

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

Assigning through IT Shop Requests

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

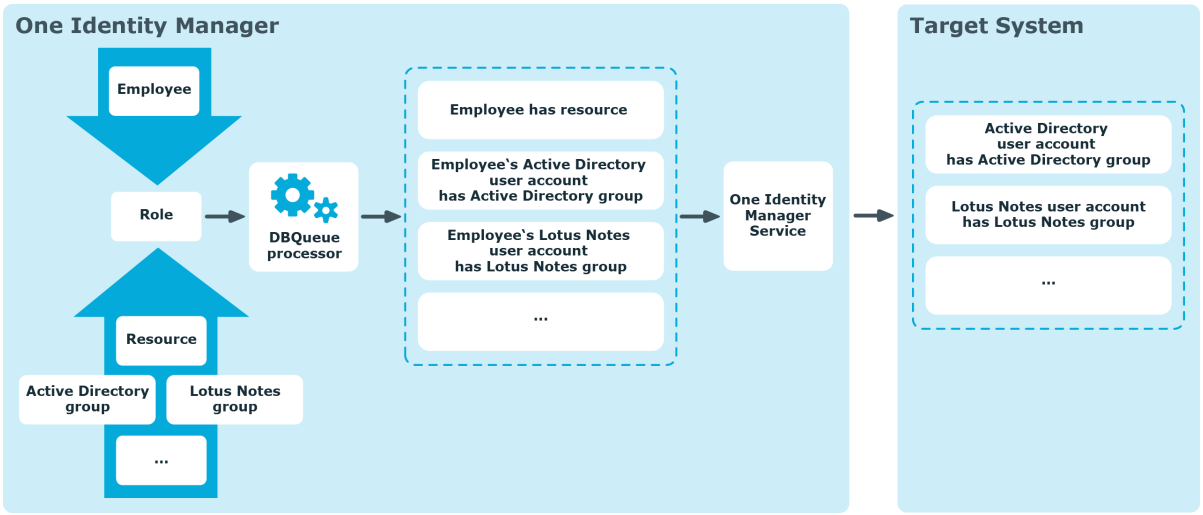
Figure 9: Assignment Schema through Requests



Basics for Calculating Inheritance

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

Figure 10: Overview of Inheritance Calculation



Calculating Inheritance through 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

View	Meaning
ORG	Graphical representation of business roles

NOTE: Because the views are sections 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. The complete transitive closure of the tree is stored in the table BaseTreeCollection. As transitive closure, all roles that the given role is inherited from, are labeled in a full list. Depending on the section of the table BaseTree there is a corresponding, so-called Collection table containing the transitive closure section.

The following relations apply in the table BaseTreeCollection:

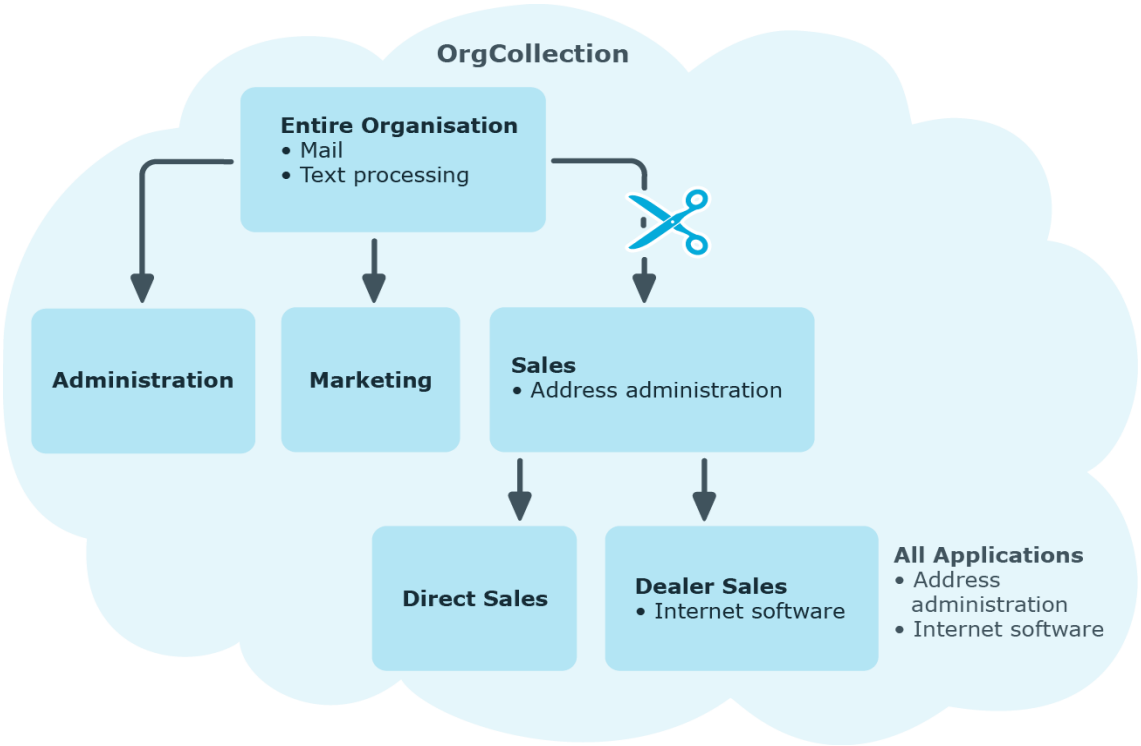
- UID_Org is the role that inherits.
- UID_ParentOrg is the role that passes down inheritance.

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. The

recursive loop is also included in the transitive closure as base element. That means that each role inherits from itself.

Each role in a role hierarchy must be related to the table `OrgRoot` ("Role classes"). `BaseTreeRoot` is the anchor for transitive closures. Meaning transitive closures are only ever formed for one role class. Roles from different role classes may not be in one and the same role hierarchical or point to each other through a parent-child relationship.

Figure 11: Representation of a Hierarchical Structure with a Transitive Closure using the Example of an OrgCollection



A role inherits everything that is assigned to its the parents in the transitive closure including those things 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 table `BaseTree` and also previous structures according to the table `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.

The column `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, this assignment, however, will not be put in effect.

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

Table 4: Possible Values for Column XOrigin

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

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.
- Define mutually exclusive roles if required.

  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

- Permit Assignments of Employees, Devices, Workdesks and Company Resources on page 19
- Specifying the Direction of Inheritance on page 20
- Using Business Roles to Limit Inheritance on page 21
- Define Inheritance Exclusion for Business Roles on page 44

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

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

Assignable Company Resource	Members in Roles	
	Employees	Workdesks
Azure Active Directory Subscriptions	possible (assigns to all an employee's Azure Active Directory user accounts, for which group inheritance is authorized)	-
Disabled Azure Active Directory service plans	possible (assigns to all an employee's Azure Active Directory user accounts, for which group inheritance is authorized)	-
Unix groups	possible (assigns to all an employee's Unix groups)	-
System roles	possible	possible
Subscribable reports	possible	-
Applications	possible	possible

Related Topics

- Assigning Business Roles to Company Resources on page 35

Permit 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:

- Assignment allowed

  This option specifies whether assignments of respective object types to roles of this role class are allowed in general.

- Direct assignment allowed

  Use this option to specify whether respective object types can be assigned directly to roles of this role class. Set this option if, for example, resources are assigned to departments, cost centers or locations over the assignment form in the Manager.

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

Example

To assign employees in Manager directly to a business role, set the option **Assignment allowed** and the option **Direct assignment allowed** on the role class "business role" for the entry "employees".

If employees can only obtain membership in a business role through the IT Shop, set the option **Assignment allowed** but not the option **Direct assignment allowed** on the role class "business role" for the entry "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 the option **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 the column **Allow direct assignments** to specify whether a direct assignment is allowed.

   NOTE: You can only reset the option **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 the option **Inherited top down** to specify top-down inheritance.
- Set the option **Inherited bottom up** to specify bottom-up inheritance.

Detailed information about this topic

- Direction of Inheritance within a Hierarchy on page 6
- Roles Classes on page 25

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 the option **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 the option **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. Set the option
   - **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 the option **No inheritance**.

   The employee does not inherit company resources through roles.

   NOTE: This option does not affect direct assignments! Company resource direct assignments remain assigned.
3. Save the changes.

To prevent an device from inheriting

1. Open the device's master data form.
2. Set the option **No inheritance**.

   The device does not inherit company resources through roles.

   NOTE: This option does not affect direct assignments! Company resource direct assignments remain assigned.
3. Save the changes.

To prevent a workdesk from inheriting

1. Open the workdesk's master data form.
2. Set the option **No inheritance**.

   The workdesk does not inherit company resources through roles.

   NOTE: This option does not affect direct assignments! Company resource direct assignments remain assigned.
3. Save the changes.

Related Topics

- Discontinuing Inheritance on page 8

Inheritance Exclusion: Specifying Conflicting Roles

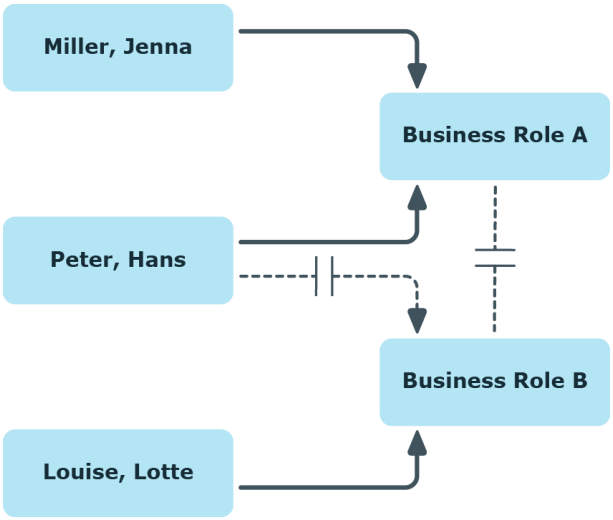
You can define conflicting roles to prevent employees, devices or workdesks from being assigned to several roles at the same time and from obtaining mutually exclusive company resources through these roles. At the same time, you specify which business roles need to be mutually exclusive. This means you 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



To configure inheritance exclusion

- Set the configuration parameter "QER\Structures\ExcludeStructures" in the Designer and compile the database.

Related Topics

- Define Inheritance Exclusion for Business Roles on page 44

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 the category **Base data | General | Configuration parameters** in the Designer.

- Roles Classes

  Role classes form the basis of mapping from hierarchical roles in the 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 employees to business roles that can be brought in as attestors in attestation cases when 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 the One Identity Manager to this application role. You may create other application roles as required. For more detailed information about implementing and editing application roles, see the One Identity Manager Application Roles Administration Guide.

- Approvers and Approvers (IT)

  In One Identity Manager, you can assign employees to business roles that can be brought in as approvers in approval procedures for IT Shop requests when 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 more detailed information about implementing and editing application roles, see the One Identity Manager Application Roles Administration Guide.

Detailed information about this topic

- Roles Classes on page 25
- Role Types on page 26
- Functional areas on page 26
- Attestors on page 28
- Approvers and Approvers (IT) on page 28

Roles 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 category **Business roles | Basic configuration data | Role classes**.
2. Select the role class in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
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

Property	Description
Role classes	Role class description The role class is displayed under this name in the navigation view.
Attestors	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. NOTE: This property is available if the Attestation Module is installed.
Description	Spare text box for additional explanation.
Inherited top down	Direction of inheritance top-down.
Inherited bottom-up	Direction of inheritance bottom-up
Delegable	Specifies whether memberships in roles of this role class can be delegated.
Assignment allowed	Specifies whether assignments of respective object types to roles of this role class are allowed in general.
Assignment not allowed	Specifies whether respective object types can be assigned directly to roles of this role class.

Related Topics

- Direction of Inheritance within a Hierarchy on page 6
- Permit Assignments of Employees, Devices, Workdesks and Company Resources on page 19

Role Types

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

To edit role types

1. Select the category **Business roles | Basic configuration data | Role types**.
2. Select the role type in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
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

Property	Description
Role type	Role type description
Description	Spare text box for additional explanation.

Functional areas

To analyze rule checks for different areas of your company in the context of identity audit, you can set up functional areas. Functional areas can be assigned to hierarchical roles and service items. You can enter criteria that provide information about risks from rule violations for functional areas and hierarchical roles. To do this, you specify how man 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

The risk of rule violation should be analyzed 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. Define assessment criteria for the functional areas.
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. Select the category **Business roles | Basic configuration data | Functional areas**.
2. Select the functional area in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Edit the function area master data.
4. Save the changes.

Enter the following data for a functional area.

Table 8: Functional Area Properties

Property	Description
Functional area	Description of the functional area
Parent Functional area	Parent functional area in a hierarchy. Select a parent functional area from the list in order to organize your functional areas hierarchically.
Max. number of rule violations	List of rule violation valid for this functional area. This value can be evaluated during the rule check. NOTE: This input field is available if theCompliance 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 employees to business roles that can be brought in as attestors in attestation cases when 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 the One Identity Manager to this application role. You may create other application roles as required. For more detailed information about implementing and editing application roles, see the One Identity Manager Application Roles Administration Guide.

Table 9: Default Application Roles for Attestors

User	Task
Business Role Attestors	Attestors must be assigned to the application role **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.

To specify attestors

1. Select the category **Business roles | Basic configuration data | Attestors**.
2. Select **Assign employees** in the task view.
3. Assign employees in **Add assignments**.

   - OR -

   Remove employees from **Remove assignments**.
4. Save the changes.

Approvers and Approvers (IT)

In One Identity Manager, you can assign employees to business roles that can be brought in as approvers in approval procedures for IT Shop requests when 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 more detailed information about implementing and editing application roles, see the One Identity Manager Application Roles Administration Guide.

Table 10: Default Application Roles for Approvers

User	Task
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 the application role **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 the category **Business roles | Basic configuration data | Approver**.

   - OR -

   Select the category **Business roles | Basic configuration data | Approver (IT)**.
2. Select **Assign employees** in the task view.
3. Assign employees in **Add assignments**.

   - OR -

   Remove employees from **Remove assignments**.
4. Save the changes.

How to Edit 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 Roles Classes on page 25.

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** in the task view.

   - OR -

   Click in the result list toolbar.
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 11: General Master Data for a Business Role

Property	Description
Business role	Business role name.
Short name	Short name for the business role.
Internal name	Additional identifier for the business role.
Role Classes	Role class to which the business role is assigned. The value is preset with the role classes selected in the navigation view. If a new business role is added, you can assign any role class to it.
Parent business role	Parent of business role in the hierarchy. To organize business roles hierarchically, select the parent business role in the menu. Only the business roles that belong to the same role class can be selected. Leave this field empty if the business role is at the top level of the business role hierarchy.
Role type	Select a role type from the menu. To create a new role type, click . Enter a name and description for the role type.
Role approver	Application role whose members approve IT Shop requests for members of this business role. To create a new application role, click . Enter the application role name and assign a parent application role.
Role approver	Application role whose members approve IT Shop requests for members of this business role.

Property	Description
(IT)	To create a new application role, click . Enter the application role name and assign a parent application role.
Manager	Manager responsible for the business role.
Assistant 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 . Enter the application role name and assign a parent application role. NOTE: This property is available if the Attestation Module is installed.
Department	Department to which the business role is primary assigned.
Location	Location to which the business role is primary assigned.
Cost center	Cost center to which the business role is primary assigned.
Description	Spare text box for additional explanation.
Comment	Spare text box for additional explanation.
Remarks	Spare text box for additional explanation.
Certification status	Business role certification status. You can select the following certification statuses: • New - The business role has been added to the One Identity Manager database. • Certified - The business role's master data has been granted approval by a manager. • Denied - The business role's master data has been denied approval by a manager.
Import data source	Target system or data source, from which the data set was imported.
Block inheritance	Specifies whether inheritance for this business role can be discontinued. Set this option to discontinue inheritance within the business role hierarchy.
X500 nodes	Select this option to label a cost center for exporting to an X500 schema.
Employees do not inherit	Specifies whether employee inheritance should be temporarily prevented for this business role.
Devices do	Specifies whether device inheritance should be temporarily prevented for

Property	Description
not inherit	this business role.
Workdesks do not inherit	Specifies whether workdesk inheritance should be temporarily prevented for this business role.
Dynamic roles not allowed	Specifies whether a dynamic role can be created for the business role.

Related Topics

- Roles Classes on page 25
- Role Types on page 26
- Approvers and Approvers (IT) on page 28
- Attestors on page 28
- Using Business Roles to Limit Inheritance on page 21
- Creating Dynamic Roles on page 42

Business Role Address Data

Enter the following master data for contacting the business role.

Table 12: Business Role Address Data

Property	Description
Address	Business role mail address
Street	Street or road.
Building	Building
Zip code	Zip code.
Town	City.
Country	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.
State	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.
Phone	Business role telephone number.

Property	Description
Quick dial	Telephone short entry (without code).
Room	Room.
Comment (room)	Spare text box for additional explanation.

Functional Area and Risk Assessment

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

Table 13: Master Data of a Business Role's Functional Area

Property	Description
Functional area	Department functional area This data is required for department's risk assessment. For more information, see Functional areas on page 26.
Risk index (calculated)	A risk index is calculated for the department risk assessment based on assigned company resources. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. For more detailed information, see the .One Identity Manager Risk Assessment Administration Guide
Transparency index	Specifies how well you can trace department assignments. Use the slider to enter a value between 0 and 1. 0 ... no transparency 1 ... full transparency
Max. number of rule violations	Specify how many rule violations are permitted for this department. The value can be evaluated when compliance rules are checked. NOTE: This property is only available if the Compliance Rules Module is installed.
Turnover for this unit	Business roles turnover.
Earnings for this unit	Business roles earnings.

User Defined Master Data for Business Roles

Additional company specific information. Use the 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 workdesks
4. Assign the objects in **Add assignments**.

   - OR -

   Remove the objects in **Remove assignments**.
5. Save the changes.

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

Related Topics

- Permit Assignments of Employees, Devices, Workdesks and Company Resources on page 19
- Assigning Business Roles to Company Resources on page 35
- Creating Dynamic Roles on page 42

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: Whether secondary assignment of company resources is possible depends on the role classes.

  If an employee, device or a workdesk fulfill 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

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

Company Resource	Available in Module
LDAP groups	LDAP Module
Notes groups	IBM Notes Module
SAP groups	SAP R/3 User Management module Module
SAP profiles	SAP R/3 User Management module Module
SAP roles	SAP R/3 User Management module Module
Structural profiles	SAP R/3 Structural Profiles Add-on Module
BI analysis authorizations	SAP R/3 Analysis Authorizations Add-on 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

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 -

   Remove company resource in **Remove assignments**.
5. Save the changes.

Detailed information about this topic

- Basics for Assigning Company Resources on page 10
- Permit Assignments of Employees, Devices, Workdesks and Company Resources on page 19

Related Topics

- Possible Company Resource Assignments on page 17
- Assigning Employees, Devices and Workdesks to Business Roles on page 34
- Creating Dynamic Roles on page 42

Analyzing Role Memberships and Employee Assignments

The report "Overview of all Assignments" is displayed for certain objects, for example, permissions, 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.

Example

- 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, all roles are determined in which there are employees with this group.
- If the report is created for a compliance rule, all roles are determined in which there are employees with 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**.
- Use the **Used by button** in the report's toolbar to select the role class (department, location, business role or IT Shop structure) for which you determine if roles exist in which there are 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. In the report's toolbar, click to open the legend.
- 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 for Report "Overview of all assignments"

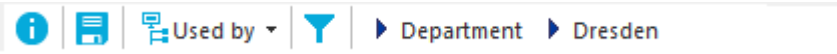


Table 15: Meaning of Icons in the Report Toolbar

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

Setting Up IT Operating Data

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

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

Example:

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

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain A. Specify the 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 specify IT operating data

1. Select the category **Business roles | <Role class>**.
2. Select the role in the result list.
3. Select **Edit IT operating data** in the task view and enter the following data.

Table 16: IT Operating Data

Property	Description
Organization/Business role	Department, cost center, location or business role for which the IT operating data is valid.
Effects on	IT operating data application scope. The IT operating data can be used for a target system or a defined account definition. ***To specify an application scope*** a. Click → next to the text box. b. Select the table under **Table**, which maps the target system or the table `TSBAccountDef` for an account definition. c. Select the concrete target system or concrete account definition under **Effects on**. d. Click **OK**.
Column	User account property for which the value is set. Columns using the script template `TSB_ITDataFromOrg` in their template are listed. For more detailed information, see the One Identity Manager Target System Base Module Administration Guide.
Value	Concrete value which is assigned to the user account property.

4. 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

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

Target system type	IT Operating Data
Azure Active Directory	Groups can be inherited
	Identity
	Privileged user account
	Change password the next time you log in
Cloud target system	Container (per target system)
	Groups can be inherited
	Identity
	Privileged user account
Unix-based target system	Login shell
	Groups can be inherited
	Identity
	Privileged user account
Exchange Online	Groups can be inherited
G Suite	Organizational unit
	Groups can be inherited
	Privileged user account
	Change password the next time you log in

Modifying 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 the effect of a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the database in the case of each affected column in each affected database.

Prerequisites

- The IT operating data of a business role was changed.

  - OR -

- The default values in the IT operating data template were modified for an account definition.

NOTE: If the assignment of an employee to a primary business role changes, the templates are automatically executed.

To execute the template

1. 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 applied to the object property after modifying the IT operating data.
Selection	Specifies whether the modification is applied to the user account.

4. Mark all the object properties in the **selection** column that will be given the new value.
5. Click **Apply**.

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

Additional Tasks for Managing Business Roles

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which 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 or 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 Permit Assignments of Employees, Devices, Workdesks and Company Resources on page 19.

NOTE: The task **Create dynamic role** is only available for business roles, which do not have the option **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 the category **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** in the task view.
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 30

Assign 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 the category **Organizations | Departments**, **Organizations | Cost centers** or **Organizations | Locations**.
2. Select the role in the result list.
3. Select **Assign business roles** in the task view.

4. Assign business roles in **Add assignments**.

   The selected role is assigned to all business roles as primary department, cost center or location.

   - OR -

   Remove the business roles in **Remove assignments**.
5. Save the changes.

Define 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 the category **Business roles | <Role class>**.
2. Select a business role in the result list.
3. Select **Edit conflicting business roles** in the task view.
4. Assign the business roles that are mutually exclusive to the selected business role in **Add assignments**.

   - OR -

   Remove the conflicting business roles that are no longer mutually exclusive in **Remove assignments**.
5. Save the changes.

Detailed information about this topic

- Inheritance Exclusion: Specifying Conflicting Roles on page 22

Assigning Extended Properties

You can assign extended properties to business roles. Extended properties are meta objects that cannot be mapped directly in the 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 assignments to extended properties in **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 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

Report	Description
Overview of all assignments	This report finds all the roles in which employees from the selected business roles are also members.
Show historical memberships	This report lists all members of the selected business role and the length of their membership.
Show products still to be approved	The report shows all products for a business role whose requests can be approved by the business role's members.
Business roles with high risk level	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 the category **My One Identity Manager**.

Related Topics

- Analyzing Role Memberships and Employee Assignments on page 37

2

Role Mining in One Identity Manager

Business roles can be formed in two ways:

- Role modeling is 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 the configuration parameter "QER\Org\RoleMining" in the Designer.

NOTE: To use Analyzer for analyzing permissions, at least the Target System Base Module must be installed.

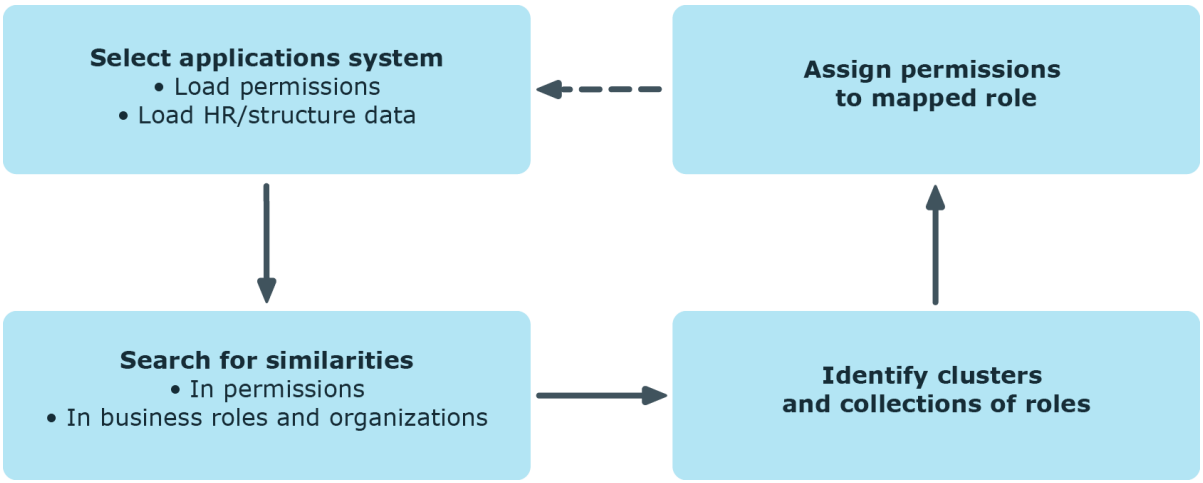
Cluster Analysis as Basis for Role Mining

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 the 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

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

Menu Items

Table 19: Meaning of Items in the Menu Bar

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

Customizing Program Settings

To change the program settings

- Select **Database | Settings...** from the menu.

Table 20: Program Settings

Setting	Meaning
Automatically close analysis information window on completion	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.
Show permissions weighting	Set this option to also display a weighting for the permissions.
Role naming template	Define a template for role names. This is used when to format new role names in predefined analysis methods. The template support following variables: %sequence% Sequential number %object% Name of first object in cluster %property% Name of first property in cluster

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

Analysis Methods	Description
Use the wizard to select analysis data	The output is collected with a wizard. For more information, see Selecting Analysis Data with the Wizard on page 51.
Active Directory Employee Permissions	Permissions are analyzed of all employees with Active Directory group memberships. For more information, see Predefined Analyzes on page 53. NOTE: Analysis methods are available if Active Directory Module is available.
Active	Permissions are analyzed of all employees with Active Directory

Analysis Methods	Description
Directory Employee Permissions and Departments	group memberships. Departments with Active Directory groups are also included in the analysis. For more information, see Predefined Analyzes on page 53. NOTE: Analysis methods are available if Active Directory Module is available.

- Verify the analysis results. For more information, see Analysis Evaluation on page 54.
- Create a new business role if required and assigned employees to them. Add the suggested changes to the One Identity Manager database. For more information, see Transferring Changes on page 56.

Selecting Analysis Data with 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. Select **Select data with wizard** on the Analyzer's start screen.
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 the selection method **Structures**.
        b. Click **Next**.
        c. Select the organization or business role to analyze in the **Structures** list.

           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

Icon	Meaning
	Show indirectly assigned employees.
	Show directly assigned employees
	Show employees from child nodes

d. Click **Next**.

- Filter wizard

  You define a condition which is 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 table "Person". For more information about using the wizard, see .One Identity Manager User Guide for One Identity Manager Tools User Interface and Default Functions

- Menu

  The list displays all the employees in the One Identity Manager database. Use **SHIFT + SELECTION** or **CTRL + SELECTION** 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. User **CTRL + SELECT** to multi-select target systems.
6. Click **Next**.
7. Specify the analysis methods. The following methods are available.

Table 23: Analysis Method

Analysis Methods	Description
Simple cluster analysis/Complex cluster analysis	Permissions are grouped with new business roles using cluster analysis methods and assigned employees. The Analyzer supports role mining through two different cluster analysis methods, which differ in the way they calculate the distances between clusters.
Decision hierarchy	Permissions are grouped into new business roles in a decision hierarchy and employees are assigned to it. The number of group members is taken as the decision criteria.

Analysis Methods	Description
Structure assignment	You may use existing role structure, for example, organizational structures from ERP systems. The use of existing structures, for example, organizational structure from ERP systems, is possible.
Permissions analysis	Employees 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.

8. Click **Next**.
9. (Optional) To reuse the configuration at a later time, set the option **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 54.
11. Create a new business role if required and assigned employees to them. Add the suggested changes to the One Identity Manager database. For more information, see Transferring Changes on page 56.

Predefined Analyzes

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

The following predefined analyses are provided:

- Active Directory Employee Permissions

  Permissions are analyzed of all employees with Active Directory group memberships.
- Active Directory Employee Permissions and Departments

  Permissions are analyzed of all employees with Active Directory group memberships. Departments with Active Directory groups are also included in the analysis.

To start predefined analysis

1. Select **Active Directory Employee Permissions** or **Select 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.

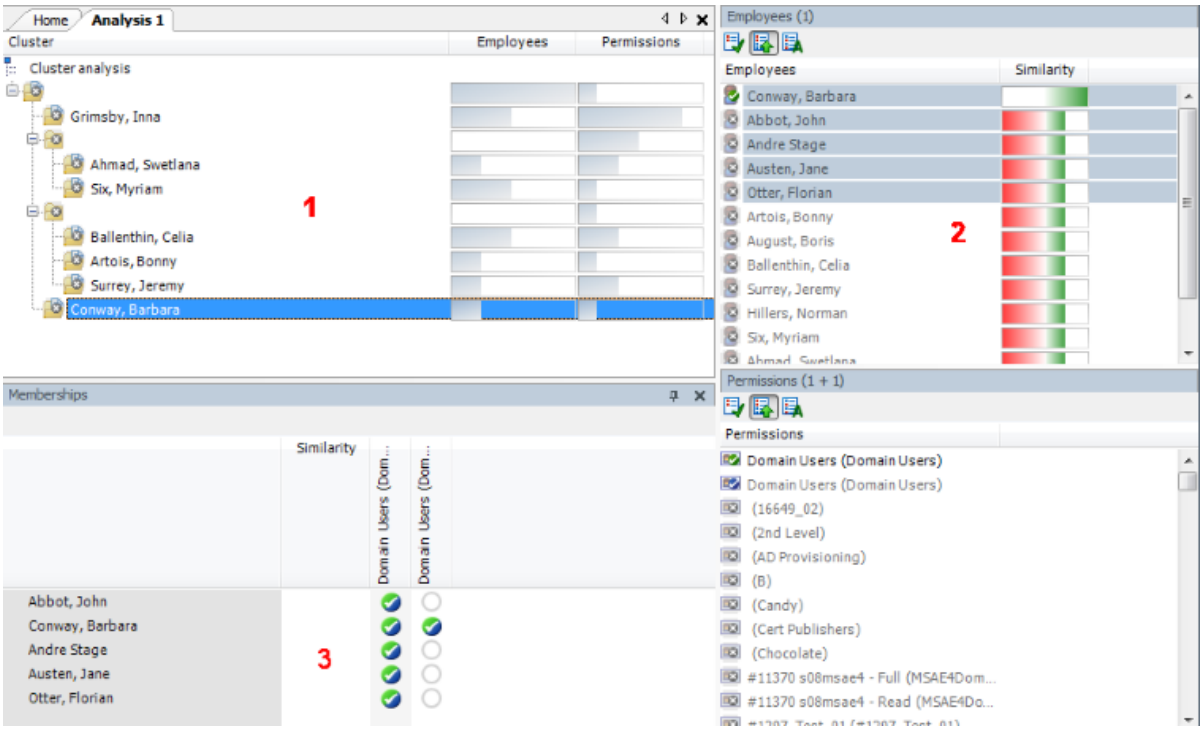
   Analysis data is displayed depending on the program settings. Click **Expand...** to see detailed information. Click **Finish** to close the dialog box. The results of the analysis are subsequently displayed. For more information, see Analysis Evaluation on page 54.

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



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% and is represented with maximized bars.

Table 24: Meaning of Items in the Context Menu in View 1

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

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

Context Menu Item	Meaning
Add to business role	Adds employee/permissions to the hierarchy of the selected business role.
Remove from business role	Removes employee/permissions from the hierarchy of the selected business role.
Compare	Compares employees with each other. The result is displayed in view 3.

Context Menu Item	Meaning
Mark assignments	Marks employee/permissions assignments in the hierarchy.
Properties	Shows other properties of active objects.

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 context menu items **Insert** and **Add recursively** to do this. You can delete business roles from the data transfer using the context menu item **Remove**.
2. Select **Database | Save to database...** from menu to start the data transfer wizard and click **Next** to continue.
3. Select the role class under which the business role will be created in the One Identity Manager database.

   Use Add a new role to create a new role class.

4. Select the save options.

Table 26: Save Options for Data

Save Option	Meaning
Delete existing objects in role class	Deletes current objects in the selected role class from the One Identity Manager database.
Business roles do not inherit	Disables inheritance of assignments by business roles. NOTE: After you have checked the assignments, remove the option **Employee do not inherit** from the business roles. Use the program "Manager" to do this.
Delete direct assignments	Removes direct permissions assignments to the employees' user accounts. **WARNING: 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.**
Attest new roles	New business roles must go through an attestation case. NOTE: This function is only available if the Attestation Module is installed.

5. Click **Finished** to save the data.

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

Index

R

T

U