One Identity Manager 9.2

Business Roles Administration Guide

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 Azure Active Directory tenants. You can add identities to single business roles as members. Identities obtain their company resources through these assignments when One Identity Manager is appropriately configured.

NOTE: The Business Roles Module must be installed as a prerequisite for managing business roles in One Identity Manager. For more information about installing, see the *One Identity Manager Installation Guide*.

The One Identity Manager components for managing business roles are available if the **QER | Org** configuration parameter is set.

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

  NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

One Identity Manager users for business roles

The following users are used for the administration of business roles.

Table 1: Users

User	Tasks
Business roles administrators	Administrators must be assigned to the **Identity Management | Business roles | Administrators** application role.

User	Tasks
	Users with this application role:
	- Create and edit business roles.
	- Assign company resources to business roles.
	- Attest business roles' main data.
	- Administrate application roles for role approvers, role approvers (IT), and attestors.
	- Set up other application roles as required.
Business Role Attestors	Attestors must be assigned to the **Identity Management | Business roles | Attestors** application role 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 main data for these business roles but not edit them.
	NOTE: This application role is available if the module Attestation Module is installed.
Business Role Approvers	Approvers must be assigned to the **Identity Management | Business roles | Role approvers** application role 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 **Identity Management | Business roles | Role approvers (IT)** application role 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.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.
	One Identity Manager administrators:

User	Tasks
	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required.
	• Create system users and permissions groups for non role-based login to administration tools in the Designer as required.
	• Enable or disable additional configuration parameters in the Designer as required.
	• Create custom processes in the Designer as required.
	• Create and configure schedules as required.
Additional managers	The additional managers must be assigned to the **Identity Management	Business roles| Additional managers** application role or to a child application role. Users with this application role: • Have permission to manage business roles.

Hierarchical role structure basic principles

Business role are arranged hierarchically. Assigned company resources are inherited by members through these hierarchies. Company resource assignments are not made to individual identities, 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.

Related topics

- Inheritance directions within a hierarchy on page 9
- Discontinuing inheritance on page 11

Inheritance directions within a hierarchy

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

- Top-down inheritance

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

- Bottom-up inheritance

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

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

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

Example: Assigning company resources top-down

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

Figure 1: Assignment through top-down inheritance

Entire Organisation
- Mail
- Text processing

Administration

Marketing

Sales
- Address administration

Direct Sales

Dealer Sales
- Internet software

All Software
- Mail
- Text processing
- Address administration
- Internet software
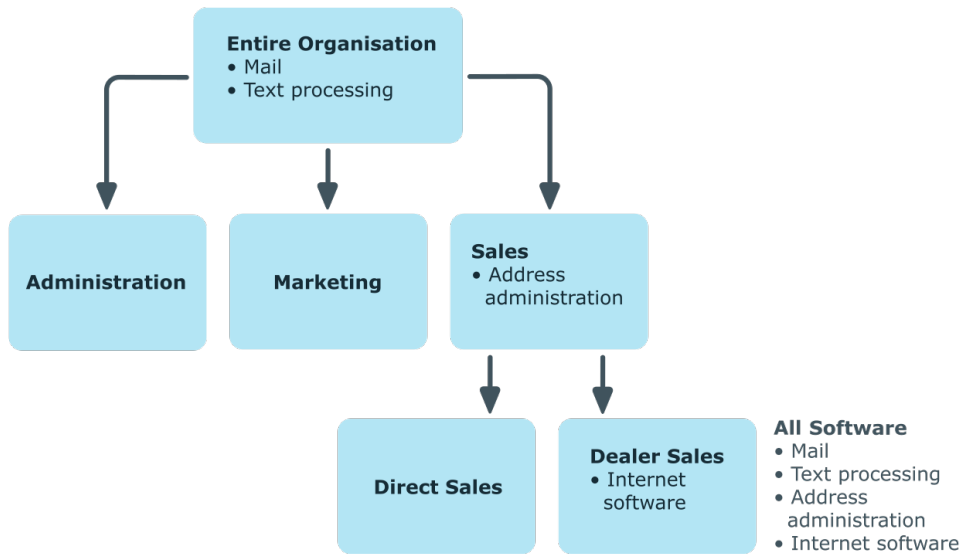
Example: Assigning company resources bottom-up

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

Figure 2: Assignment through bottom-up inheritance
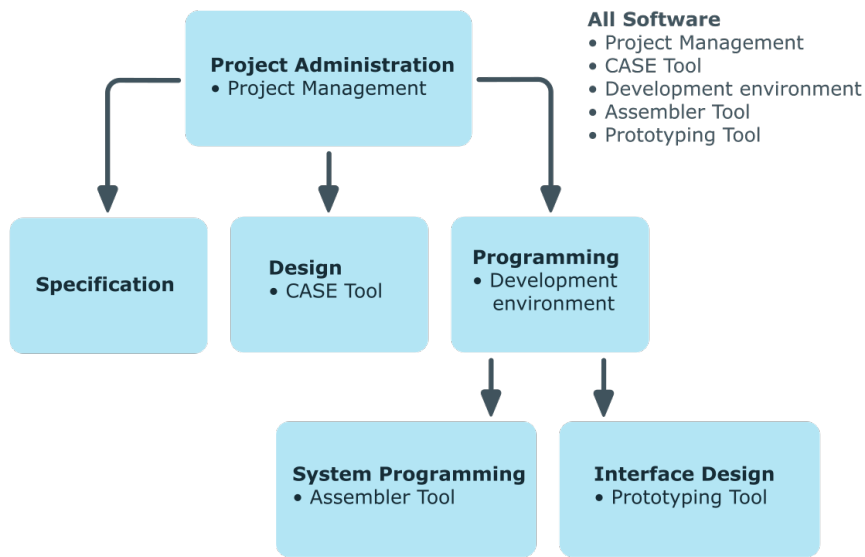
Discontinuing inheritance

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

- Roles marked with the **Block inheritance** option do not inherit any assignments from parent levels in top-down inheritance. It can, however, pass on its own directly assigned company resources to lower level structures.

- In bottom-up inheritance, the role labeled with the "Block inheritance" option inherits all assignments from lower levels in the hierarchy. However, it does not pass any assignments further up the hierarchy.

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

Example: Discontinuing inheritance top-down

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

Figure 3: Discontinuing inheritance top-down
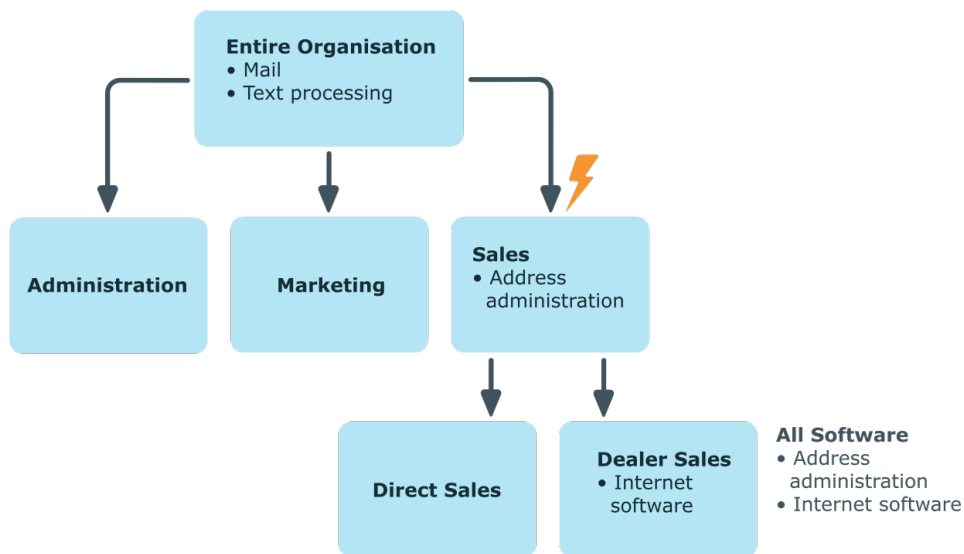
Example: Discontinuing inheritance bottom-up

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

Figure 4: Discontinuing inheritance bottom-up
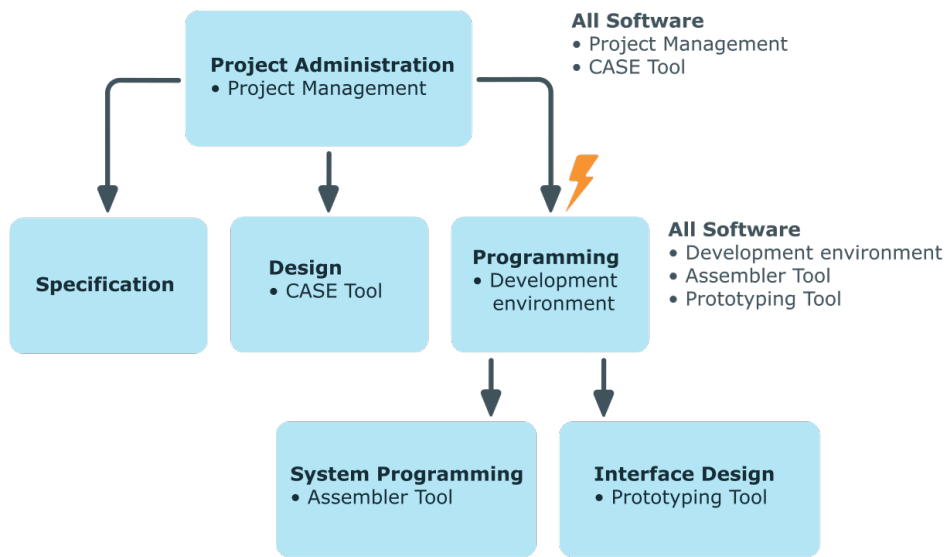
Related topics

- Blocking inheritance using business roles on page 27

Basic principles for assigning company resources

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

Assignments types are:

- Direct company resource assignments
- Indirect company resource assignments
- Assigning company resources through dynamic roles
- Assigning company resources through IT Shop requests

Direct company resource assignments

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

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

Indirect company resource assignments

In the case of indirect assignment of company resources, identities, devices, and workdesks are arranged in departments, cost centers, locations, business roles, or application roles. The total of assigned company resources for an identity, 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 example of an identity

Secondary assignment of company resources

You make a secondary assignment by classifying an identity, a device, or a workdesk within a role hierarchy. Secondary assignment is the default method for assigning and inheriting company resources through roles. In the role classes , specify whether a secondary assignment of company resources to identities, device, and workdesk is possible.

Figure 7: Secondary assignment inheritance schema
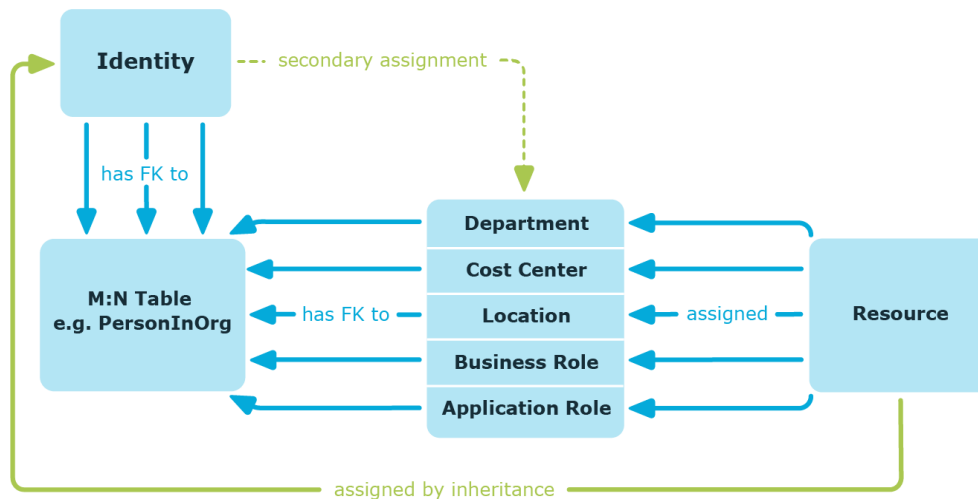
Related topics

- Allowing assignments of identities, devices, workdesks, and company resources to business roles on page 25

Primary assignment of company resources

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

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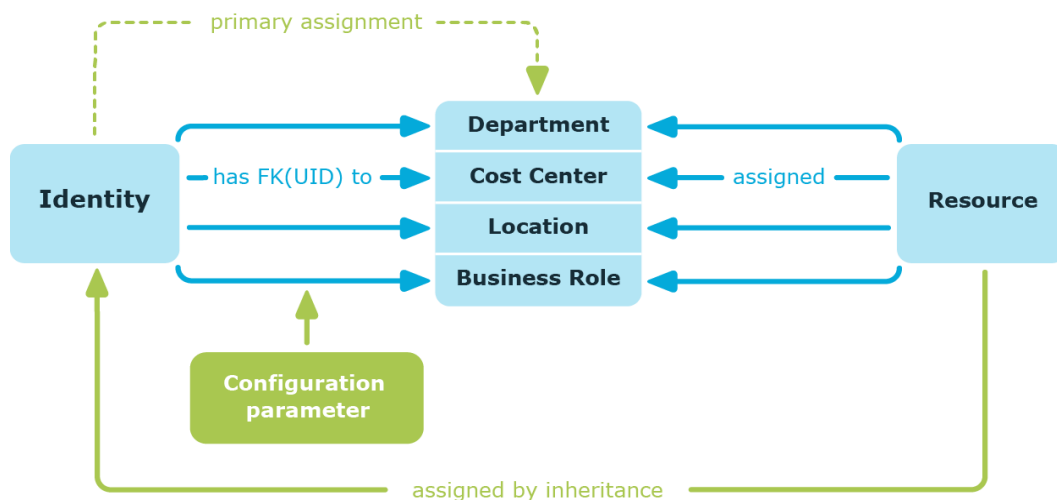
NOTE: Changes to the configuration parameter result in the inheritance data being recalculated! That means: if the primary assignment is disabled at a later date, the inheritance data created in this way will be removed from the database.

Table 2: Configuration parameters for primary assignment

Configuration parameter	Effect when set
QER | Structures | Inherite | Person	Identities can inherit through primary assignment.
QER | Structures | Inherite | Person | FromOrg	Identities inherit assignments from their primary business role (`Person.UID_Org`).
QER | Structures | Inherite | Hardware	Devices can inherit through primary assignment.
QER | Structures | Inherite | Hardware | FromOrg	Devices inherit assignments from their primary business role (`Hardware.UID_Locality`).
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 company resources through dynamic roles

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

Assigning company resources through IT Shop requests

Assignment through the IT Shop is a special case of indirect assignment. Add identities 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 identities after approval is granted. Role memberships can be requested through the IT Shop as well as company resources.

Figure 9: Schema of assignment by requests
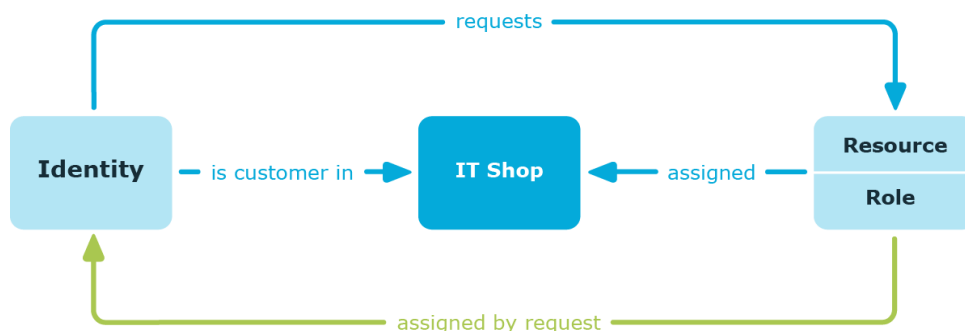
Basics of calculating inheritance

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

Figure 10: Overview of inheritance calculation
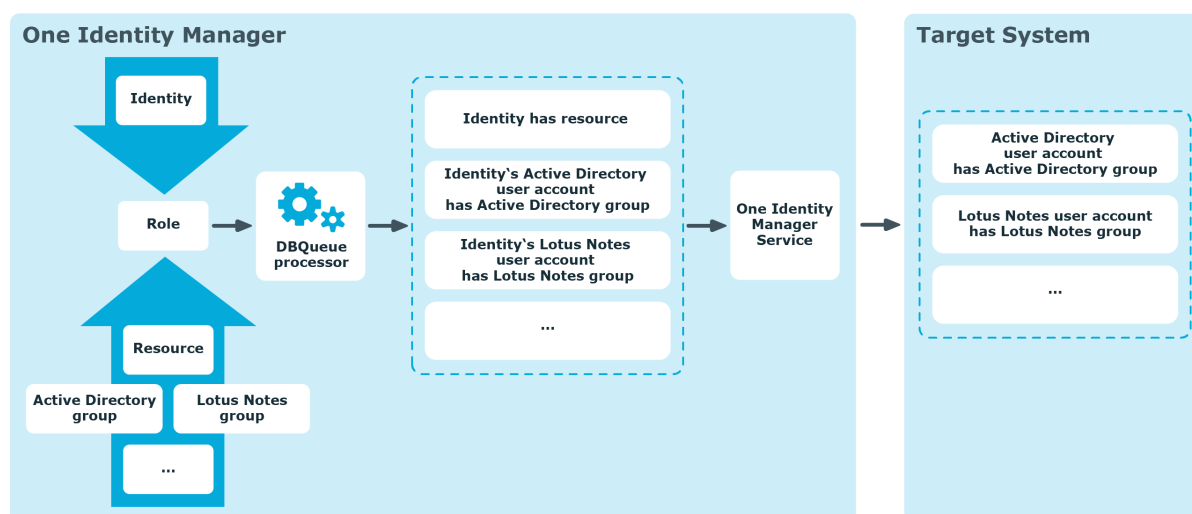
Calculating inheritance by hierarchical roles

Identities, devices, and workdesks can only be members in roles that are extensions of the `BaseTree` table. These role are display in views, each of which represents a certain of the `BaseTree` table.

Table 3: BaseTree table views

View	Meaning
ORG	Graphical representation of business roles

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

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

The following relations apply in the `BaseTreeCollection` table:

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

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

Each role inherits from itself.

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

Figure 11: Hierarchical role structure based on an OrgCollection
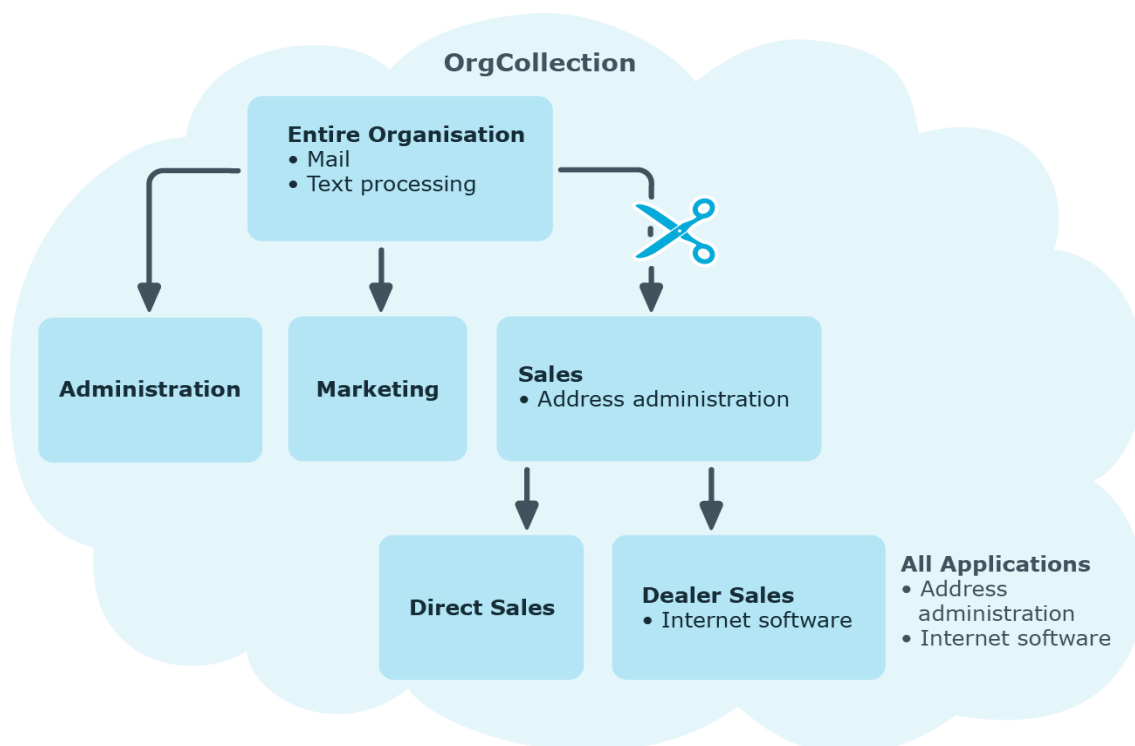
A role inherits everything that is assigned to its parents in the role hierarchy including those it assigned to itself. If the number of roles from which the role has inherited something changes, the assigned objects are recalculated for all members of this role. If the number of assigned objects of one class changes, the objects assigned in this class are recalculated for all members of the role. If a software application is assigned to a parent role, the members of the `BaseTreeHasApp` table are recalculated.

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

Calculation of assignments

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

That means:

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

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

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**	Assigned by assignment request and directly.
1	0	1	0	**10**	Assigned by assignment request and indirectly.
1	0	1	1	**11**	Assigned by assignment request, directly, and indirectly.
1	1	0	0	**12**	Assigned by assignment request and through dynamic roles.
1	1	0	1	**13**	Assigned by assignment request, directly, and through dynamic roles.
1	1	1	0	**14**	Assigned by assignment request, indirectly, and through dynamic roles.
1	1	1	1	**15**	Assignment request, direct, indirect, and through dynamic roles.

Special features of inheriting assignments though a role hierarchy

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

> **Example:**
>
> An Active Directory group assignment was requested for the "Sales" business role. The "Sales EMEA" child business role inherits this assignment. In the `OrgHasADSGroup` table, `XOrigin` is set as follows:
>
> - Business role "Sales": `XOrigin='8'` (assignment resource)
> - Business role "Sales EMEA": `XOrigin='2'` (indirect assignment)

Effectiveness of assignments

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

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

Preparing business roles for company resource assignments

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

- Specify whether identities, 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 identities, devices, or workdesks.

- If required, define roles that are mutually exclusive.

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

Detailed information about this topic

Possible assignments of company resources through business roles

Identities, devices, and workdesks can inherit company resources though indirect assignment. To do this, identities, devices, and workdesks may be members of as many roles as required. Identities, 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 identities, 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	
	Identities	Workdesks
Resources	Possible	-
Account definitions	Possible	
Groups of custom target systems	Possible (assigns to all an identity's custom defined target systems user accounts, for which group inheritance is authorized)	-
System entitlements of custom target systems	Possible (assigns to all an identity's custom defined target systems user accounts, for which system entitlement inheritance is authorized)	-
Active Directory groups	Possible (assigns to all an identity's Active Directory user accounts and Active Directory contacts, for which Active Directory group inheritance is authorized)	-
SharePoint groups	Possible (assigns to all an identity's	-

Assignable Company Resource	Members in Roles	
	Identities	**Workdesks**
	SharePoint user accounts for which SharePoint group inheritance is authorized)	
SharePoint roles	Possible (assigns to all an identity's SharePoint user accounts for which SharePoint role inheritance is authorized)	-
LDAP groups	Possible (assigns to all an identity's LDAP user accounts for which LDAP group inheritance is authorized)	-
Notes groups	Possible (assigns to all an identity's Notes user accounts for which Notes group inheritance is authorized)	-
SAP groups	Possible (assigns to all an identity's SAP user accounts, in the same SAP system and for which SAP group inheritance is authorized)	-
SAP profiles	Possible (assigns to all an identity's SAP user accounts, in the same SAP system and for which SAP profile inheritance is authorized)	-
SAP roles	Possible (assigns to all an identity's SAP user accounts, in the same SAP system and for which SAP role inheritance is authorized)	-
SAP parameters	Possible (assigns to all an identity's SAP user accounts in the same SAP system)	-
Structural profiles	Possible (assigns to all an identity's SAP user accounts, in the same SAP system and for which structural profile inheritance is authorized)	-
BI analysis authorizations	Possible (assigns to all an identity's BI user accounts, in the same system and for which group inheritance is authorized)	-
Azure Active Directory groups	Possible (assigns to all an identity's Azure Active Directory user accounts for which Azure Active Directory group	-

Assignable Company Resource	Members in Roles	
	Identities	**Workdesks**
	inheritance is authorized)	
Azure Active Directory administrator roles	Possible (assigns to all an identity's Azure Active Directory user accounts for which Azure Active Directory administrator role inheritance is authorized)	-
Azure Active Directory subscriptions	Possible (assigns to all an identity's Azure Active Directory user accounts for which Azure Active Directory subscription inheritance is authorized)	-
Disabled Azure Active Directory service plans	Possible (assigns to all an identity's Azure Active Directory user accounts for which disabled Azure Active Directory service plans inheritance is authorized)	-
Cloud groups	Possible (assigns to all an identity's user accounts for which cloud group inheritance is authorized)	-
Cloud system entitlements	Possible (assigns to all an identity's user accounts for which cloud system entitlement inheritance is authorized)	-
Unix groups	Possible (assigns to all an identity's Unix user accounts for which Unix group inheritance is authorized)	-
E-Business Suite permissions	Possible (assigns to all an identity's E-Business Suite user accounts, in the same E-Business Suite system and for which E-Business Suite group inheritance is authorized)	-
PAM user groups	Possible (assigns to all an identity's PAM user accounts for which PAM group inheritance is authorized)	-
Google Workspace products and SKUs	Possible (assigns to all an identity's Google Workspace user accounts, in the same customer and for which Google Workspace products and SKU inheritance is authorized)	-
Google Workspace groups	Possible (assigns to all an identity's Google Workspace user accounts, in the same customer and for which	-

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

Related topics

Allowing assignments of identities, devices, workdesks, and company resources to business roles

The default method for assigning company resources is through secondary assignment. For this, identities, 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 the IT Shop, dynamic roles, or system roles.

Example:

To assign identities directly to a business role in the Manager, enable the **Assignment allowed** and the **Direct assignment allowed** options on the **Identities** entry in the **Business role** role class.

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

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.

2. Select the **Configure role assignments** task.

3. Use the **Allow assignments** column to specify whether assignment is generally allowed.

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

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

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

5. Save the changes.

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 9
- Role classes for business roles on page 33

Blocking inheritance using business roles

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

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

To discontinue inheritance for business roles

1. In the Manager, in the **Organizations** category, select a business role.
2. Select the **Change main data** task.
3. Set the **Block inheritance** option.
4. Save the changes.

Related topics

- Discontinuing inheritance on page 11
- Preventing inheritance of individual business roles by identities, devices, or workdesks on page 28
- Preventing inheritance by individual identities, devices, or workdesks on page 28

Preventing inheritance of individual business roles by identities, devices, or workdesks

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

To prevent inheritance for business roles

1. In the Manager, in the **Organizations** category, select a business role.

2. Select the **Change main data** task.

3. Set one or more of the following options:

   - To prevent identities from inheriting, set the **Identities do not inherit** option.

   - To prevent devices from inheriting, set the **Devices do not inherit** option.

   - To prevent workdesks from inheriting, set the **Workdesks do not inherit** option.

4. Save the changes.

Related topics

- Blocking inheritance using business roles on page 27
- Preventing inheritance by individual identities, devices, or workdesks on page 28

Preventing inheritance by individual identities, devices, or workdesks

Inheritance of company resources can be prevented for single identities, devices, or workdesks. For example, you can use this behavior after importing to correct the imported data first and then apply inheritance afterward.

To prevent an identity from inheriting

1. In the Manager, select the identity in the **Identities** category.

2. Select the **Change main data** task.

3. Set the **No inheritance** option.

   The identity does not inherit company resources through roles.

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

4. Save the changes.

To prevent an device from inheriting

1. In the Manager, select the device in the **Devices & Workdesks > Devices** category.

2. Select the **Change main data** task.

3. Set the **No inheritance** option.

    The device does not inherit company resources through roles.

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

4. Save the changes.

To prevent a workdesk from inheriting

1. In the Manager, select the workdesk in the **Devices & Workdesks > Workdesks** category.

2. Select the **Change main data** task.

3. Set the **No inheritance** option.

    The workdesk does not inherit company resources through roles.

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

4. Save the changes.

Related topics

- Blocking inheritance using business roles on page 27
- Preventing inheritance of individual business roles by identities, devices, or workdesks on page 28

Inheritance exclusion: Specifying conflicting roles

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

> NOTE: Only roles, which are defined directly as conflicting roles cannot be assigned to the same identity (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 Alex User1 and Jo Identity are members of business role A. Toni User2 is member of business role B. Jo Identity cannot be assigned to business role B. Apart from that, One Identity Manager also prevents Alex User1 from being assigned to business role B and Toni User2 to business role A.

Figure 12: Members in conflicting roles
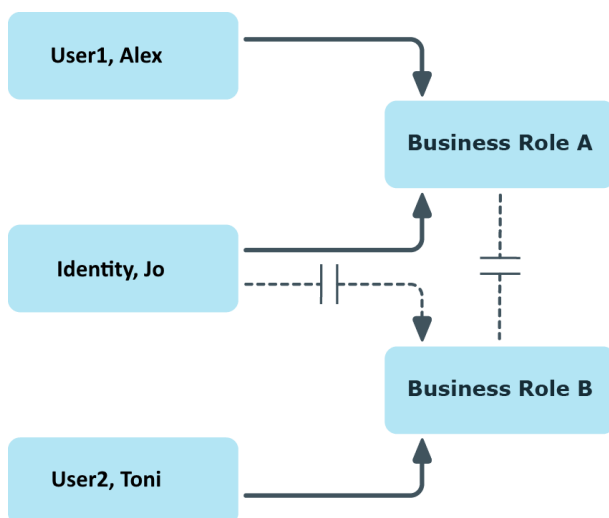
To configure inheritance exclusion

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

  NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

Related topics

- Defining inheritance exclusion for business roles on page 56

Restricting assignment of identities to multiple business roles

In certain circumstances you might want an identity to be assigned to only one business role such as, within a project structure.

To map this behavior, you can use the **No multiple assignment of identities** option. You can enable the option for role classes and role types.

- If a role class has this option enabled, an identity can be assigned to only one business role of this role class. Assignment of the identity to other business roles belonging to this role class is not allowed.

- If a role type has this option enabled, an identity can only be assigned one business role of this role type. Assignment of the identity to other business roles belonging to this role type is not allowed.

NOTE:

- Only for direct assignments of identities to business roles are verified.

- Use the **Multiple role assignments despite IsPersonAssignOnce on OrgRoot** and **Multiple role assignments despite IsPersonAssignOnce on OrgType** consistency checks to identify invalid assignments to business roles. These assignments can originate from dynamic roles or through purchase orders, for example. For more information about consistency checking, see the *One Identity Manager Operational Guide*.

- If an identity has already been assigned to multiple business roles of a role class or role type, then the option cannot be set again for this role class or role type.

Related topics

- Role classes for business roles on page 33
- Role types for business roles on page 34

Base data for business roles

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

- Configuration parameters

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

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

- Role classes

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

- Role types

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

- Functional areas

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

- Attestors

  In One Identity Manager, you can assign business roles to identities 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. For more information about attestation, see the *One Identity Manager Attestation Administration Guide*.

  A default application role for attestors is available in One Identity Manager. You may create other application roles as required. For more information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

- Role approvers and role approvers (IT)

  In One Identity Manager, you can assign business roles to identities 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. For more information, see the *One Identity Manager IT Shop Administration Guide*.

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

Detailed information about this topic

Role classes for 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. You can permit identity, device, workdesk, and company resource assignments for the role classes.

To create or edit role classes

1. In the Manager, select the **Business roles > Basic configuration data > Role classes** category.

2. In the result list, select the role class and run the **Change main data** task.

   - OR -

   Click ⊞ in the result list.

3. Edit the role class's main data.

4. Save the changes.

Enter the following main data of a role class.

Table 6: Role class properties

Property	Description
Role class	Role class description. The role class is displayed in the Manager under this name in the navigation view. Translate the given text using the 🌐 button.
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	Text field 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.
Assignments permitted	Specifies whether assignments of respective object types to roles of this role class are permitted in general. Configure the permitted assignments in the Manager using the **Configure role assignments** task.
Direct	Specifies whether respective object types can be assigned directly to

Property	Description
assignments allowed	roles of this role class. Configure the permitted assignments in the Manager using the **Configure role assignments** task.
No multiple assignment of identities	Specifies whether an identity can be assigned to only one business role of this role class. If a role class has this option enabled, an identity can be assigned to only one business role of this role class. Assignment of the identity to other business roles belonging to this role class is not allowed.

Related topics

- Inheritance directions within a hierarchy on page 9
- Allowing assignments of identities, devices, workdesks, and company resources to business roles on page 25

Assigning role types to role classes

For additional classification, you can define role types and assign them to role classes. Note the restrictions given under Role types for business roles on page 34.

To assign a role type to a role class

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

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

    To remove an assignment

    - Select the role type and click ⊘.

Related topics

- Role types for business roles on page 34
- Creating and editing role types on page 35
- Assigning role classes to role types on page 36

Role types for business roles

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

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

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

Related topics

Creating and editing role types

For additional classification, you can create and edit role types. You cannot edit default role types.

To create role types

1. In the Manager, select the **Business roles > Basic configuration data > Role types** category.

2. Click in the result list.

3. Enter the following information:

   - **Role type**: Role type name. Translate the given text using the button.
   - **Description**: (Optional) Text field for additional explanation.
   - **No multiple assignment of identities**: Specifies whether an identity is only assigned one business role of this role type. If a role type has this option enabled, an identity can only be assigned one business role of this role type. Assignment of the identity to other business roles belonging to this role type is not allowed.

     NOTE: This option does not work for departments, cost centers, and locations.

4. Save the changes.

To create role types

1. In the Manager, select the **Business roles > Basic configuration data > Role types** category.

2. Select the role type in the result list.

3. Select the **Change main data** task.

4. Edit the main data.

5. Save the changes.

Related topics

- Assigning role classes to role types on page 36
- Assigning role types to role classes on page 34

Assigning role classes to role types

For additional classification, you can define role types and assign them to role classes. Note the restrictions given under Role types for business roles on page 34.

To assign role classes to a role type

1. In the Manager, select the **Business roles > Basic configuration data > Role types** category.

2. Select the role type in the result list.

3. Select the **Assign role classes** task.

4. In the **Add assignments** pane, select the role class and assign business roles.

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

    To remove an assignment
    - Select the business role and double-click ⊘.

5. Save the changes.

Related topics

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.

Moreover, functional areas can be replaced by peer group analysis during request approvals or attestation cases.

Example: Use of functional areas

To assess the risk of rule violations for 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 create or edit a functional area

1. In the Manager, select the **Business Roles > Basic configuration data > Functional areas** category.

2. In the result list, select a function area and run the **Change main data** task.

   - OR -

   Click ▣ in the result list.

3. Edit the function area main data.

4. Save the changes.

Enter the following data for a functional area.

Table 7: Functional area properties

Property	Description
Functional area	Description of the functional area
Parent Functional area	Parent functional area in a hierarchy.
	Select a parent functional area from the list for organizing your functional areas hierarchically.
Max. number of rule violations	List of rule violation valid for this functional area. This value can be evaluated during the rule check.
	NOTE: This property is available if the Compliance Rules Module is installed.
Description	Text field for additional explanation.

Related topics

- *One Identity Manager Compliance Rules Administration Guide*

Attestors

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

In One Identity Manager, you can assign business roles to identities 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. For more information about attestation, see the *One Identity Manager Attestation Administration Guide*.

A default application role for attestors is available in One Identity Manager. You may create other application roles as required. For more information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 8: Default application roles for attestors

User	Tasks
Business Role	Attestors must be assigned to the **Identity Management	Business roles	Attestors** application role or a child application role.

User	Tasks
Attestors	Users with this application role:

> • Attest correct assignment of company resource to business roles for which they are responsible.
>
> • Can view main data for these business roles but not edit them.
>
> NOTE: This application role is available if the module Attestation Module is installed.

To add identities to default application roles for attestors

1. In the Manager, select the **Business Roles > Basic configuration data > Attestors** category.

2. Select the **Assign identities** task.

3. In the **Add assignments** pane, add identities.

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

   To remove an assignment

   • Select the identity and double-click ⊘.

4. Save the changes.

Role approvers and role approvers (IT)

In One Identity Manager, you can assign business roles to identities 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. For more information, see the *One Identity Manager IT Shop Administration Guide*.

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

Table 9: Default application roles for approvers

User	Tasks
Business Role Approvers	Approvers must be assigned to the **Identity Management | Business roles | Role approvers** application role or a child application role.
	Users with this application role:

> • Are approvers for the IT Shop.

User	Tasks
	• Approve requests from business roles for which they are responsible.
Business Role Approvers (IT)	IT role approvers must be assigned to the **Identity Management | Business roles | Role approvers (IT)** application role 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. In the Manager, select the **Business Roles > Basic configuration data > Role approvers** category.

   - OR -

   In the Manager, select the **Business Roles > Basic configuration data > Role approvers (IT)** category.

2. Select the **Assign identities** task.

3. In the **Add assignments** pane, add identities.

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

   ### *To remove an assignment*
   • Select the identity and double-click ⊘.

4. Save the changes.

Creating and 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.

To create or edit business roles

1. In the Manager, select the **Business roles > <role class>** category.

2. In the result list, select a business role and run the **Change main data** task.

   - OR -

   Click in the result list.

3. Edit the business role's main data.

4. Save the changes.

Related topics

General main data for business roles

Enter the following main data of a business role.

Table 10: General main data of a business role

Property	Description
Business role	Business role name. Translate the given text using the ⊕ button.
Short name	Short name for the business role.
Internal name	Additional identifier for the business role.
Role class	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.
Full name	Complete name of business roles including parent business roles. Translate the given text using the ⊕ button.
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 (IT)	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.
Manager	Manager responsible for the business role.
2nd Manager	Deputy business role manager.

Property	Description
Additional manager	Application role for a group of managers and deputies who manage this business role.
	To create a new application role, click 🖹+. Enter the application role name and assign a parent application role.
Attestors	Applications role whose members are authorized to approve attestation cases for this 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	Text field for additional explanation.
Comment	Text field for additional explanation.
Remarks	Text field for additional explanation.
Certification status	Business role certification status. You can select the following certification statuses:
	• **New**: The business roles was newly added to the One Identity Manager database.
	• **Certified**: The business role main data was granted approval by the manager.
	• **Denied**: The business role main data was denied approval by the manager.
	The certification status can be set depending on the result of regular attestations.
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.
Identities do not inherit	Specifies whether identity inheritance should be temporarily prevented for this business role.
Devices do not inherit	Specifies whether device inheritance should be temporarily prevented for this business role.

Property	Description
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

Address information for business roles

Enter the following main data of contacting the business role.

Table 11: Business role address data

Property	Description
Address	Business role mail address
Street	Street or road.
Building	Building
Zip code	Zip code.
City	City.
Country	Country. You require this to determine the identity'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 identity'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)	Text field for additional explanation.

Functional areas and risk assessment for business roles

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

Table 12: Main data of a business role's functional area

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

Related topics

- Functional areas on page 37

Customizing main data for business roles

Enter any custom master data. Use the Designer to customize display names, formats, and templates for the input fields.

Table 13: Custom main data for a support team

Property	Description
Spare field no. 01 ... Spare field no. 10	Additional company-specific information.
Spare date no. 01 ... Spare date no. 03	Additional company-specific information.

Assigning identities, devices, and workdesks to business roles

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

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

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

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

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

   To remove an assignment
   - Select the object and double-click ⊘.
5. Save the changes.

Related topics

- Allowing assignments of identities, devices, workdesks, and company resources to business roles on page 25

Assigning business roles to company resources

The default method of assigning identities, devices, and workdesks is indirect assignment. This allocates an identity, a device or a workdesk to business roles, cost centers, or locations. The total of assigned company resources for an identity, 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 identity, 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 identity, device or a workdesk fulfills the requirements of a dynamic role, the object is added dynamically to the corresponding company structure and can obtain company resources through it.

- Primary assignment

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

You must assign company resources to business roles, cost centers, or locations so that identities, 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 company resource assignments

Company resource	Available in Module
Resources	always
Account definitions	Target System Base Module
Groups of custom target systems	Target System Base Module
System entitlements of custom target	Target System Base Module

Company resource	Available in Module
systems	
Active Directory groups	Active Directory Module
SharePoint groups	SharePoint Module
SharePoint roles	SharePoint Module
LDAP groups	LDAP Module
Notes groups	Domino Module
SAP groups	SAP R/3 User Management Module
SAP profiles	SAP R/3 User Management Module
SAP roles	SAP R/3 User Management Module
SAP parameters	SAP R/3 User Management Module
Structural profiles	SAP R/3 Structural Profiles Add-on Module
BI analysis authorizations	SAP R/3 Analysis Authorizations Add-on Module
E-Business Suite permissions	Oracle E-Business Suite Module
System roles	System Roles Module
Subscribable reports	Report Subscription Module
Software	Software Management Module
Azure Active Directory groups	Azure Active Directory Module
Azure Active Directory administrator roles	Azure Active Directory Module
Azure Active Directory subscriptions	Azure Active Directory Module
Disabled Azure Active Directory service plans	Azure Active Directory Module
Unix groups	Unix Based Target Systems Module
Cloud groups	Cloud Systems Management Module
Cloud system entitlements	Cloud Systems Management Module
PAM user groups	Privileged Account Governance Module
Google Workspace groups	Google Workspace Module
Google Workspace products and SKUs	Google Workspace Module
SharePoint Online groups	SharePoint Online Module
SharePoint Online roles	SharePoint Online Module

Company resource	Available in Module
OneLogin roles	OneLogin Module

To add company resources to a hierarchical role

1. In the Manager, select the **Business roles > <role class>** category.

2. Select the role in the result list.

3. Select the task to assign the corresponding company resource.

4. In the **Add assignments** pane, assign company resources.

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

   #### To remove an assignment

   - Select the company resource and double-click ✅.

5. Save the changes.

Detailed information about this topic

- Basic principles for assigning company resources on page 13
- Allowing assignments of identities, devices, workdesks, and company resources to business roles on page 25

Related topics

- Possible assignments of company resources through business roles on page 22
- Assigning identities, devices, and workdesks to business roles on page 45
- Creating dynamic roles for business roles on page 54

Analyzing role memberships and identity 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 identities 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 identities with this resource.
>
> - If the report is created for a group or another system entitlement, all roles are determined in which there are identities with this group or system entitlement.
>
> - If the report is created for a compliance rule, all roles are determined in which there are identities who violate this compliance rule.
>
> - If the report is created for a department, all roles are determined in which identities of the selected department are also members.
>
> - If the report is created for a business role, all roles are determined in which identities of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the **Overview of all assignments** report.

- Click the 🔲 **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain identities 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 identities 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 identities 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 identities for tracking. This creates a new business role to which the identities are assigned.

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

🛈 | 💾 | 🔲 Used by ⌄ | 🔻 | ▶ Department ▶ Dresden
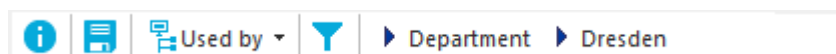
Table 15: Meaning of icons in the report toolbar

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 operational data for business roles

To create user accounts for an identity with the **Full managed** manage level, you need to know which IT operating data is required. The operating data required for each specific target system is defined with its business roles, departments, locations, or cost centers. An identity 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 identity in department A obtains a default user account in the domain A. In addition, certain identities in department A obtain administrative user accounts in the domain A.

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

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

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

To define IT operating data

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

To specify an application scope

    a. Click ➔ next to the field.

    b. Under **Table**, select the table that maps the target system for select the TSBAccountDef table or an account definition.

    c. Select the specific target system or account definition under **Effects on**.

    d. Click **OK**.

- **Column**: Select the user account property for which the value is set.

  In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For more information about this, see the *One Identity Manager Target System Base Module Administration Guide*.

- **Value**: Enter a fixed value to assign to the user account's property.

5. Save the changes.

It operating data for target systems

The IT operating data necessary in the One Identity Manager default configuration for automatically creating or changing identity 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 16: 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 type
	Privileged user account
Microsoft Exchange	Mailbox database
LDAP	Container
	Groups can be inherited
	Identity type
	Privileged user account
Domino	Server
	Certificate

Target system type	IT operating data
	Template for mail file
	Identity type
SharePoint	Authentication mode
	Groups can be inherited
	Roles can be inherited
	Identity type
	Privileged user account
SharePoint Online	Groups can be inherited
	Roles can be inherited
	Privileged user account.
	Authentication mode
Custom target systems	Container (per target system)
	Groups can be inherited
	Identity type
	Privileged user account
Azure Active Directory	Groups can be inherited
	Administrator roles can be inherited
	Subscriptions can be inherited
	Disabled service plans can be inherited
	Identity type
	Privileged user account
	Change password at next login
Cloud target system	Container (per target system)
	Groups can be inherited
	Identity type
	Privileged user account
Unix-based target system	Login shell
	Groups can be inherited
	Identity type
	Privileged user account
Oracle E-Business Suite	Identity type
	Groups can be inherited
	Privileged user account.

Target system type	IT operating data
SAP R/3	Identity type
	Groups can be inherited
	Roles can be inherited
	Profiles can be inherited
	Structural profiles can be inherited
	Privileged user account.
Exchange Online	Groups can be inherited
Privileged Account Management	Authentication provider
	Groups can be inherited
	Identity type
	Privileged user account
Google Workspace	Organization
	Groups can be inherited
	Products and SKUs can be inherited
	Admin roles assignments can be inherited
	Identity type
	Privileged user account.
	Change password at next login
OneLogin	Roles can be inherited
	Identity type
	Privileged user account.
	Licensing state
	OneLogin group

Modify IT operating data

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

Prerequisites

- The IT operating data of a business role have been changed.

  - OR -

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

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

To run the template

1. In the Manager, select the **<target system type> > Basic configuration data > Account definitions > Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Run templates** task.

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

   - **Old value**: Value of the object property before changing the IT operating data.

   - **New value**: Value of the object property after changing the IT operating data.

   - **Selection**: Specifies whether the new value is copied to the user account.

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

5. Click **Apply**.

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

Creating dynamic roles for business roles

Use this task to define dynamic roles for individual business roles. Dynamic roles are used to specify role memberships dynamically. Identities, devices, and workdesks are not permanently assigned to a role, just when they fulfill certain conditions. A check is performed regularly to assess which identities (devices or workdesks) fulfill these conditions. This means the role memberships change dynamically. For example, company resources can be assigned dynamically to all identities in a business role in this way; if an identity 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 identities, devices, and workdesks to role classes must be permitted. If necessary, further configuration settings need to be made.

NOTE: The **Create dynamic role** task is only available for business roles that do not have the **Dynamic roles not allowed** option set.

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

To create a dynamic role for a business role

1. In the Manager, select the **Business roles > <role class>** category.

2. Select a business role in the result list.

3. Select the **Create dynamic role** task.

4. Enter the required main data.

5. Save the changes.

To edit a dynamic role

1. In the Manager, select the **Organizations > <role class> > Dynamic roles** category.

2. Select a business role in the result list.

3. Open the business role's overview form.

4. In the **Dynamic roles** form element, click on the name of the dynamic role.

5. Select the **Change main data** task.

6. Edit the dynamic role's main data.

7. Save the changes.

Related topics

- General main data for business roles on page 41
- Allowing assignments of identities, devices, workdesks, and company resources to business roles on page 25

Assigning departments, cost centers, and locations to business roles

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 main 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. In the Manager, select the **Organizations > Departments**, **Organizations > Cost centers**, or **Organizations > Locations** category.

2. Select the role in the result list.

3. Select the **Assign business roles** task.

4. In the **Add assignments** pane, assign business roles.

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

5. Save the changes.

Related topics

- General main data for business roles on page 41

Defining inheritance exclusion for business roles

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

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

To configure inheritance exclusion

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

  NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

To define inheritance exclusion for a business role

1. In the Manager, select the **Business roles > <role class>** category.

2. Select a business role in the result list.

3. Select **Edit conflicting business roles**.

4. In the **Add assignments** pane, assign business roles that are mutually exclusive to the selected business role.

   - OR -

   In the **Remove assignments** pane, 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 29

Assigning extended properties to business roles

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

To specify extended properties for a business role

1. In the Manager, select the **Business roles > <role class>** category.

2. Select the business role in the result list.

3. Select the **Assign extended properties** task.

4. In the **Add assignments** pane, assign extended properties.

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

   To remove an assignment

   - Select the extended property and double-click ⊘.

5. Save the changes.

Creating assignment resources for application roles

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. In the Manager, select the **Business roles > <role class>** category.

2. Select a business role in the result list.

3. Select the **Create assignment resource** task.

   This starts a wizard that takes you through the steps for adding an assignment resource.

NOTE: Business roles associated with an assignment resource cannot be deleted until the associated assignment resource is deleted.

Dynamic roles for business roles with incorrectly excluded identities

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

- The dynamic role condition does not apply.

  For example, this might occur if the dynamic role condition was changed after an identity was entered in the exclude list.

  - OR -

- The excluded identity is also assigned to the role in another way

  such as through inheritance or direct assignment.

Check these entries and correct the assignments.

To check conflicting entries of business roles in the exclusion list

1. In the Manager, select the **Business Roles > Troubleshooting > Dynamic roles with potentially incorrect excluded identities** category.

2. Select the dynamic role in the result list.

3. Select the **Exclude identities** task.

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

For more information about editing the dynamic roles' exclusion list, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- Creating dynamic roles for business roles on page 54

Certification of business roles

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

The certification status of business roles can be set manually or by regular attestation. To set certification status by attesting, configure the attestation policies accordingly.

To manually change the certification status of a business role

1. In the Manager, edit the business role's main data.
2. In the **Certification status** field, enter the required value.
3. Save the changes.

To change the certification status of business roles by attestation

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

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

Attestation and certification is started automatically for business roles that were added with the Analyzer tool if the **QER | Attestation | OrgApproval** configuration parameter is set.

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

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

Detailed information about this topic

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 17: Reports about business roles

Report	Description
Overview of all assignments	This report finds all the roles in which identities 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 Manager in the **My One Identity Manager** category.

Related topics

- Analyzing role memberships and identity assignments on page 48

Role mining in One Identity Manager

Business roles can be formed in two ways:

- Role modeling as described in Managing business roles on page 6.

- Role mining, by analyzing existing access permissions.

Analyzer uses the One Identity Manager program 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 identities assigned in them

- Manual analysis of certain identity 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 use role mining in One Identity Manager

- In the Designer, set the **QER | Org | RoleMining** configuration parameter.

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 the Analyzer with help of mathematical algorithm tries to find single clusters, meaning identities 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. Permissions analysis can then be used to assign permissions to these role structures. Lastly, role structures can be freely defined and assignment of permissions and identities can be manually evaluated based on existing permissions.

Figure 14: Cluster analysis methods in the Analyzer
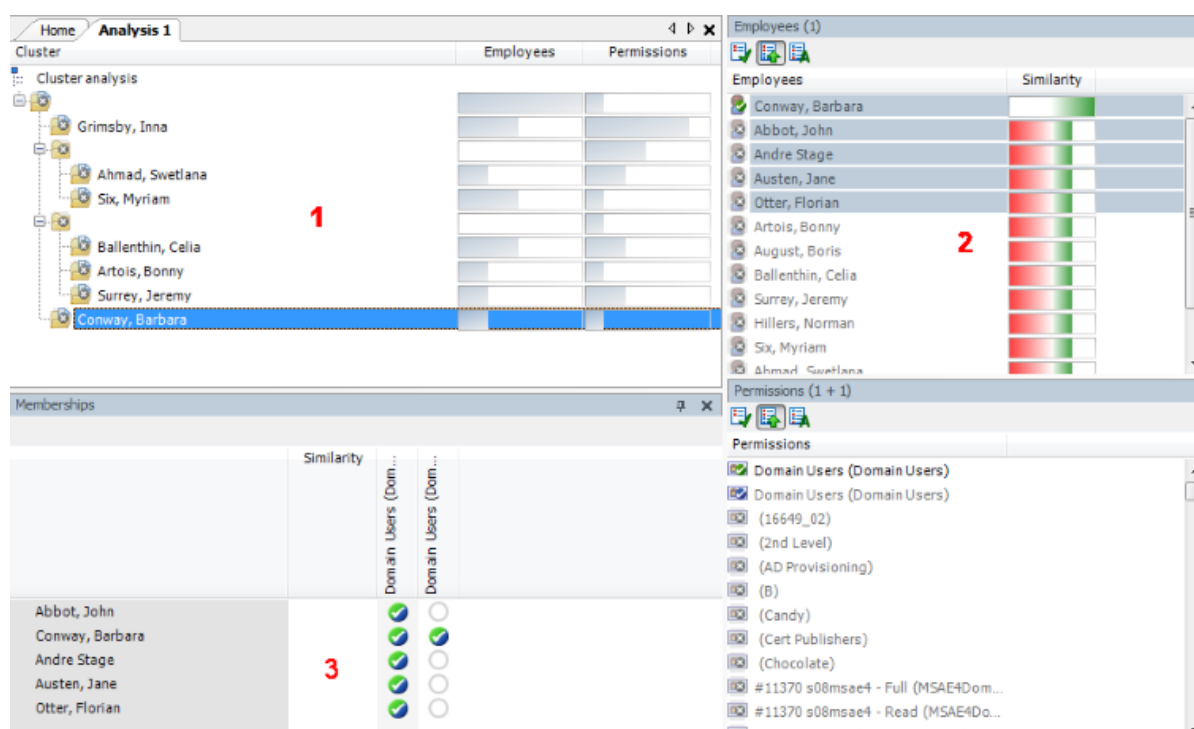
In clustering methods, Analyzer calculates a frequency distribution from user permissions in the different application systems, like Active Directory, HCL Domino, or SAP R/3. Certain permissions may have a higher weighting in comparison to others. The number of a permissions' members can, for example, 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. For example, this information can be used to replace direct permissions assignments with indirect assignments therefore reducing the administration effort.

Analyzer menu items

Table 18: Meaning of items in the menu bar

Menu	Menu item	Meaning	Shortcut
Database	New connection	Establishes a 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 identity/permissions assignment.	Ctrl + U
	Next assignment	Jumps to next identity/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.	

Analyzer program settings

To change the program settings in the Analyzer

1. In the Analyzer, select the **Database > Settings** menu item.

2. Customize the following settings.

   - **Common language**: Language for formatting data, such as data formats, time formats or number formats.

   - **Other user interface language**:Language for the user interface. The initial program login uses the system language for the user interface. Changes to the language settings take effect after the program has been restarted.The language is set globally for all One Identity Manager programs, which means the language setting does not have to be configured for each program individually.

   - **Automatically close analysis information window on completion**: If this option is set and analyses are predefined, the information window is closed at the end of the analysis. If the option is not set, the information window is shown. Click the **Finished** button to close the window.

   - **Show permissions weighting**: Set this option to additionally 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 the first object in the cluster

     %property%: Name of the first property in the cluster

3. Save the settings with **OK**.

Running an analysis in the Analyzer

Use the Analyzer to perform the following steps:

1. Specify the analysis method.

   - **Selecting analysis data using the wizard**: The initial data is collected using a wizard.

   - **Active Directory Identity Permissions**: The permissions of all identities with Active Directory group memberships are analyzed.

     NOTE: Analysis methods are available if the Active Directory Module is installed.

- **Active Directory Identity Permissions and Departments**: The permissions of all identities with Active Directory group memberships are analyzed. Departments with Active Directory groups are also included in the analysis.

  NOTE: Analysis methods are available if the Active Directory Module is installed.

- **LDAP Identity Permissions**: The permissions of all identities with LDAP group memberships are analyzed.

  NOTE: Analysis methods are available if the LDAP Module is installed.

2. Verify the analysis results.

3. Create a new business role if required and assign the identities. Add the suggested changes to the One Identity Manager database.

Detailed information about this topic

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 identities 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 with the wizard

1. Start the Launchpad and log in to the One Identity Manager database.

2. Open the Launchpad and select **Analyze business roles** in the **Manage** section. This starts the Analyzer program.

3. On the Analyzer's start page, select the **Select data with wizard** analysis method and click **Start**.

   This starts the wizard.

4. On the start page, you specify the identities for analysis. Select one of the following selection categories and click **Next**.

   - **Structures**: Identities can be selected through organizations and business roles contained in One Identity Manager.

1. In the **Structures** list, select the organization or business role for analysis.

2. The identities assigned to this structure are displayed in the **Identities** list. Use the Show directly/indirectly assigned identities buttons in the title bar to filter the identities.

Table 19: Icons for filtering identities

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

- **Query wizard**: Define the condition used to find the identities 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 the *One Identity Manager User Guide for One Identity Manager Tools User Interface*.

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

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

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

6. On the **Select analysis method** page, you specify the analysis method. The following methods are available.

Table 20: Analysis methods

Analysis method	Description
Simple cluster analysis/Complex cluster analysis	Permissions are grouped into new business roles using cluster analysis methods and identities 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.
Decision hierarchy	Permissions are grouped into new business roles in a decision hierarchy and the identities are assigned. The number of group members is taken as the decision criteria.

Analysis method	Description
Structure assignment	The permissions are assigned to an existing structure hierarchy. The use of existing structures, for example, organizational structure from ERP systems, is possible.
Permissions analysis	Identity permissions are analyzed with the help of permissions analysis. Business roles are freely defined and assignments of permissions and identities are evaluated manually based on the existing permissions.

7. On the last page you start the analysis.

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

   b. On the last page, click **Finish** to start the analysis.

      This loads the analysis data and starts the analysis. The results of the analysis are then displayed in the Analyzer.

8. Verify the analysis results.

9. Create a new business role if required and assign the identities. Add the suggested changes to the One Identity Manager database.

Related topics

Run predefined analysis

The following predefined analyses are provided:

- **Active Directory Identity Permissions**: The permissions of all identities with Active Directory group memberships are analyzed.

  | NOTE: Analysis methods are available if the Active Directory Module is installed.

- **Active Directory Identity Permissions and Departments**: The permissions of all identities with Active Directory group memberships are analyzed. Departments with Active Directory groups are also included in the analysis.

  | NOTE: Analysis methods are available if the Active Directory Module is installed.

- **LDAP Identity Permissions**: The permissions of all identities with LDAP group memberships are analyzed.

  | NOTE: Analysis methods are available if the LDAP Module is installed.

To start a predefined analysis

1. Start the Launchpad and log in to the One Identity Manager database.

2. Open the Launchpad and select **Analyze business roles** in the **Manage** section. This starts the Analyzer program.

3. On the Analyzer's start page, select the predefined analysis procedure and click **Start**.

   This loads the analysis data and starts analysis immediately. This may take some time, depending on the amount of data. The results of the analysis are then displayed in the Analyzer.

   > NOTE: If you have disabled the **Automatically close analysis information window on completion** program setting, information about the analysis is displayed in the **Cluster analysis** window. Click **Expand** to see detailed information. Click **Finish** to close the dialog.

4. Verify the analysis results.

5. Create a new business role if required and assign the identities. Add the suggested changes to the One Identity Manager database.

Related topics

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 identity assignments and business role permissions directly. You can create new business roles with the Analyzer and assign them directly to identities. This makes adding and moving identities 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
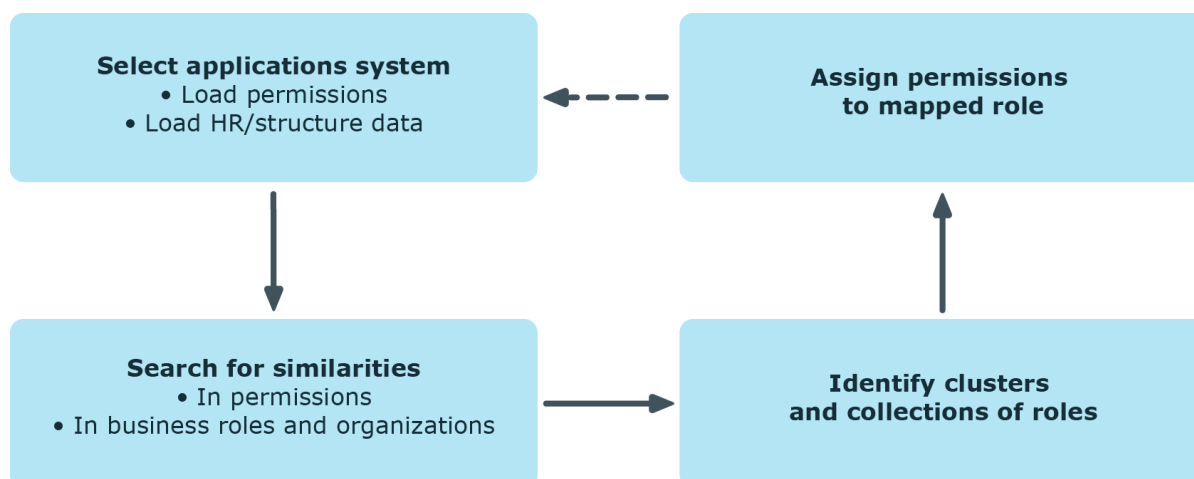
On the left, the clusters found by the analysis are displayed hierarchically on a tab. The nodes mapped here are named through the first identity found when analysis data is selected with wizards. The naming of predefined analysis methods follows specified rules in the program settings. You can change names using **F2** or **Rename** in the context menu.

The number of occurrences is displayed graphically in the columns <Identities> and <Permissions>. The display is normed in both columns, which means the group with the highest number of identities or permissions assigned to it corresponds to 100 percent and is represented with maximized bars.

Table 21: 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 (**Database> > Settings** menu).
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 identities (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 identity's permissions for the analyzed target systems separately. A permissions weighting is displayed depending on the program settings.

Table 22: Meaning of items in the context menu in view 2

Context Menu Item	Meaning
Add to business role	Adds identity/permissions to the hierarchy of the selected business role.
Remove from business role	Removes identity/permissions from the hierarchy of the selected business role.
Compare	Compares identities with each other. The result is displayed in view 3.
Mark assignments	Marks identity/permissions assignments in the hierarchy.
Properties	Shows other properties of active objects.

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

To compare identity memberships

- Select identities in the right pane (2) using **Ctrl + select** or **Shift + select**.
- Click **Compare** in the context menu to start comparing.

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

Applying changes from the analysis

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

To transfer changes to the One Identity Manager database

1. In the Analyzer, in the hierarchy mark the business roles you want to transfer.

   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 > Commit to database** from menu to start the data transfer wizard and click **Next** to continue.

3. On the **Save options** page, you specify the following settings:

   a. **Role class**: 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.

   b. Select the save options.

      - **Delete existing objects in role class**: This option deletes existing objects in the selected role class from the One Identity Manager database.

      - **Business roles do not inherit**: This option disables inheritance of assignments by business roles.

        NOTE: Once you have checked the assignments, remove the **Identities do not inherit** option from the business roles. Use the Manager program to do this.

      - **Delete direct assignments**: This option removes direct permissions assignments to the identities' user accounts.

        ⚠ **CAUTION: Only set this option if you have ensured that the permissions are inherited by the identities 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.

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

Related topics

- Certification of business roles on page 59

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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index