



One Identity Manager 9.0

System Roles Administration Guide

Copyright 2022 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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

One Identity Manager System Roles Administration Guide
Updated - 01 August 2022, 16:22
Version - 9.0

Contents

Managing system roles	5
One Identity Manager users for managing system roles	6
Basics of calculating the inheritance of system roles	7
Details of system role inheritance	8
Effectiveness of system roles	9
Disabled system roles	11
Creating and editing system roles	12
General main data of system roles	12
Creating and editing system role types	15
Assigning company resources to system roles	15
Assigning system roles to workdesks and employees	17
Assigning system roles to departments, cost centers, and locations	19
Assigning system roles to business roles	19
Adding system roles to the IT Shop	20
Assigning system roles directly to employees	21
Assigning system roles directly to workdesks	22
Adding system roles to system roles	23
Assigning system roles	24
Excluding system roles	24
Assigning extended properties to system roles	25
Displaying the system role overview	26
Appendix: Configuration parameters for system roles	27
Appendix: Examples of system role inheritance	28
Example of a system role hierarchy	28
Examples of inheritance paths for system roles	29
Effect of exclusion definitions for system roles	31
Special features of inheritance system roles through hierarchical roles	33
About us	36
Contacting us	36
Technical support resources	36

Index37

Managing system roles

System roles make it easier to assign company resources that are frequently required or rather that are always assigned together. For example, new employees in the finance department should be provided, by default, with certain system entitlements for Active Directory and for SAP R/3. In order to avoid a lot of separate assignments, group these company resources into a package and assign this to the new employee. The packages are referred to as system role in One Identity Manager.

Using system roles, you can group together arbitrary company resources. You can assign these system roles to employees, workdesks, or roles or you can request them through the IT Shop. Employees and workdesks inherit company resources assigned to the system roles. You can structure system roles by assigning other system roles to them.

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

One Identity Manager components for managing system roles are available if the **QER | ESet** 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 not 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*.

Detailed information about this topic

- [One Identity Manager users for managing system roles](#) on page 6
- [Basics of calculating the inheritance of system roles](#) on page 7
- [Creating and editing system roles](#) on page 12
- [Configuration parameters for system roles](#) on page 27
- [Examples of system role inheritance](#) on page 28

One Identity Manager users for managing system roles

The following users are used for setting up and administration of system roles.

Table 1: Users

User	Tasks
Employee responsible for individual company resources	<p>The users are defined using different application roles for administrators and managers.</p> <p>Users with these application roles:</p> <ul style="list-style-type: none">• Create and edit system roles.• Assign system roles to departments, cost centers, locations, business roles, or the IT Shop.• Assign system roles to employees.• Assign system roles to workdesks.
Product owners for the IT Shop	<p>Product owners must be assigned to the Request & Fulfillment IT Shop Product owners application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Approve through requests.• Edit service items and service categories under their management. <p>The Request & Fulfillment IT Shop Product owners System roles default application role can be used.</p>
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none">• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required.• Create system users and permissions groups for non role-based login to administration tools in the Designer as required.• Enable or disable additional configuration parameters in the Designer as required.• Create custom processes in the Designer as required.• Create and configure schedules as required.

Basics of calculating the inheritance of system roles

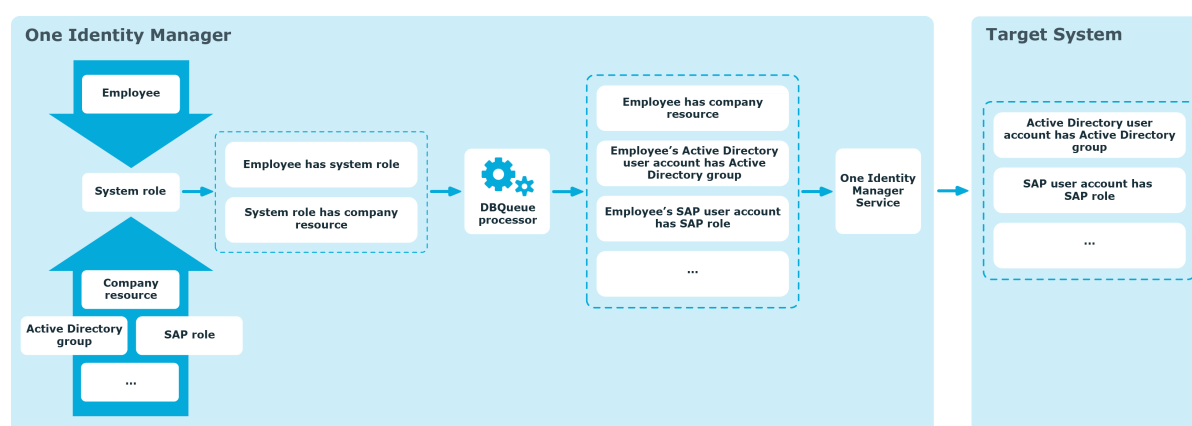
Any number of company resources and other system roles can be assigned to system roles. By assigning system roles to other system roles, you can structure system roles hierarchically. System roles can be assigned to employees and workdesks in the following ways:

- Direct assignment
- IT Shop request
- Inheritance through hierarchical roles
- Inheritance through dynamic roles

An employee (workdesk, hierarchical role) inherits all company resources that are assigned to the assigned system role. Child system roles are resolved in this case. Prerequisite is that each company resource can really be inherited.

NOTE: The employee must own a user account in this target system in order to inherit a target system entitlement.

Figure 1: Inheriting company resources through system roles



Objects assigned through inheritance are calculated by the DBQueue Processor. Tasks are added to the DBQueue when assignments relevant to inheritance are made. These tasks are processed by the DBQueue Processor and result in follow-on tasks for the DBQueue or

in processes for process component `HandleObjectComponent` in the Job queue. Resulting assignments of permissions to user accounts in the target system are inserted, modified, or deleted during process handling.

Detailed information about this topic

- [Details of system role inheritance](#) on page 8
- [Effectiveness of system roles](#) on page 9
- [Disabled system roles](#) on page 11
- [Example of a system role hierarchy](#) on page 28

Details of system role inheritance

The company resource assignments to system roles are mapped in the `ESetHasEntitlement` table.

The system role hierarchy is mapped through the `UID_ESet` - Entitlement relation. The system role hierarchy is stored in the `ESetCollection` table. All the system roles are listed that the given system role inherits from. Each role also inherits from itself.

The following relations apply in the `ESetCollection` table:

- `UID_ESet` is the system role that inherits.
- It inherits from the `UID_ESetChild` system role.

The `ESetHasEntitlement` table contains the direct assignment (`XOrigin = 1`) and all system roles that are assigned to the child system roles (`XOrigin = 2`). The company resources that are assigned to a child system role are not resolved until inheritance for employees, workdesks, and hierarchical roles is calculated.

Assignment of system roles to hierarchical roles are mapped in the `BaseTreeHasESet` table.

Employees can directly obtain system roles. Employees continue to inherit all (including inherited) the system roles belonging to all hierarchical roles of which they are members (table `PersonInBasetree`) as well as system roles of all hierarchical roles that are referenced through foreign key relations (`Person` table, `UID_BaseTree` column). Direct and indirect assignments of system roles to employees are mapped in the `PersonHasESet` table. This behavior applies in the same way to assignments of system roles to workdesks.

Detailed information about this topic

- [Examples of inheritance paths for system roles](#) on page 29

Effectiveness of system roles

By assigning system roles to employees, workdesks, or hierarchical roles, an employee may obtain company resources, which should not be assigned in this combination. To prevent this, you can declare mutually exclusive system roles. To do this you specify which system role of a pair of system roles, should be take effect if both are assigned. No company resources are inherited by the system role which is not effective.

Prerequisite

- The **QER | Structures | Inherit | ESetExclusion** configuration parameter is set.

In the Designer, 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 not 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*.

It is possible, to assign employees, workdesks, and company resources directly, indirectly, or by IT Shop request to an excluded system role. This can be done at any time. One Identity Manager subsequently determines whether the assignment takes effect and the company resources are inherited.

NOTE:

- You cannot define a pair of mutually exclusive system roles. That means, the definition "System role A excludes System role B" AND "System role B excludes System role A" is not permitted.
- You must declare each system role to be excluded from a system role separately. Exclusion definitions cannot be inherited.

The effect of the assignments is mapped in the PersonHasESet, BaseTreeHasESet, and WorkdeskHasESet tables through the XIsInEffect column.

NOTE: If a company resource assigned to an excluded system role, is assigned directly or indirectly to an employee, or workdesk, the exclusion definition does not affect this company resource. The exclusion definition only applies to the system roles.

Example: Effectiveness of system roles

- The "Marketing" system role contains all the software applications and permissions for triggering requests.
- The "Finance" system role contains all the software applications and permissions for instructing payments.

- The "Controlling" system role contains all the software applications and permissions for verifying invoices.

Jo User1 directly assigns the system role "Marketing". They obtain the "Finance" system role and the "Controlling" system role through an IT Shop request. Jo User1 obtains all the system roles without an exclusion definition and therefore the associated permissions.

By using suitable controls, you want to prevent an employee from being able to trigger a request and also pay invoices. That means, the "Finance" and "Marketing" are system roles mutually exclusive. An employee that checks invoices may not be able to make invoice payments as well. That means, the "Finance" and "Controlling" system roles are mutually exclusive.

Table 2: Specifying mutually exclusive system roles (table ESetExcludesESet)

Effective business role	Excluded System Role
Finance	Marketing
Controlling	Finance

Table 3: Effective assignments

Employee	Assigned system role	Effective business role
Pat Identity1	Marketing	Marketing
Jan User3	Marketing, finance	Finance
Jo User1	Marketing, finance, controlling	Controlling
Chris User2	Marketing, Controlling	Marketing, Controlling

Only the "Controlling" system role is in effect for Jo User1. If the "Controlling" system role is removed from Jo User1, the "Finance" system role assignment is reinstated.

Chris User2 retains the "Marketing" and "Controlling" system roles because there is no exclusion defined between the two system roles. That means that the employee is authorized to trigger request and to check invoices. If you want to prevent that as well, define further exclusion for the "Controlling" system role.

Table 4: Excluded system roles and effective assignments

Employee	Assigned system role	Excluded System Role (UID_ ESetExcluded)	Effective business role
Chris User2	Marketing		Controlling
	Controlling	Finance Marketing	

Detailed information about this topic

- [Effect of exclusion definitions for system roles on page 31](#)
- [Special features of inheritance system roles through hierarchical roles on page 33](#)
- [Excluding system roles on page 24](#)

Disabled system roles

System roles can be disabled to temporarily to prevent, for example, employees and workdesks from inheriting their company resources. If a system role is disabled, the DBQueue Processor recalculates inheritance of its company resources. Existing assignments to employees and workdesks are removed. The disabled system role remains assigned however, the assignment no longer has any effect (`PersonHasESet.XIsInEffect = 0`). Once the system role is re-enabled, company resource inheritance is recalculated again. The company resources contained in the system role are assigned to employees and workdesks.


You cannot request a disabled system role in the Web Portal but you can assign a disabled system role directly to employees, workdesks, hierarchical roles, dynamic roles, and IT Shop shelves.

Related topics

- [General main data of system roles on page 12](#)

Creating and editing system roles

To create or edit a system role

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list. Select the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the system role's main data.
4. Save the changes.

Detailed information about this topic

- [General main data of system roles](#) on page 12
- [Creating and editing system role types](#) on page 15
- [Assigning company resources to system roles](#) on page 15
- [Assigning system roles to workdesks and employees](#) on page 17
- [Excluding system roles](#) on page 24
- [Assigning extended properties to system roles](#) on page 25
- [Displaying the system role overview](#) on page 26
- [Configuration parameters for system roles](#) on page 27

General main data of system roles

Enter the following data for a system role.

Table 5: System role main data

Property	Description
Display name	Name for displaying the system roles in One Identity Manager tools.

Property	Description
System role	Unique identifier for the system role.
Internal product name	An additional internal name for the system role.
System role type	Specifies the type of company resources, which comprise the system role.
Service item	In order to use a service item within the IT Shop, assign a service item to it or add a new service item. For more information about service items, see the <i>One Identity Manager IT Shop Administration Guide</i> .
System role manager	<p>Manager responsible for the system role. Assign any new employee. This employee can edit system role main data. They can be used as attestors for system role properties.</p> <p>If the system role can be requested in the IT Shop, the manager will automatically be a member of the application role for product owners assigned the service item.</p>
Share date	<p>Specify a date for enabling the system role. If the date is in the future, the system role is considered to be disabled. If the date is reached, the system role is enabled. Employees inherit company resources that are assigned to the system role.</p> <p>If the share date is exceeded or no date is entered, the system role is handled as an enabled system role. Company resource inheritance can be controlled with the Disabled option in these cases.</p> <p>NOTE: Configure and enable the Share system roles schedule in the Designer to check the share date. For more information about schedules, see the <i>One Identity Manager Operational Guide</i>.</p>
Risk index (calculated)	Maximum risk index values for all company resources. The property is only visible if the QER CalculateRiskIndex configuration parameter is enabled. For more information about calculating the risk index, see the <i>One Identity Manager Risk Assessment Administration Guide</i> .
Comment	Text field for additional explanation.
Remarks	Text field for additional explanation.
Description	Text field for additional explanation.
Deactivated	<p>Specifies whether employees and workdesks inherit the company resources contained in the system role.</p> <p>If this option is set, the system role can be assigned to employees, workdesks, hierarchical roles, and IT Shop shelves. However they cannot inherit the company resources contained in the system role. The system role cannot be requested in the Web Portal.</p>

Property	Description
	If this option is not set, company resources assigned to the system role are inherited. If the option is enabled at a later date, existing assignments are removed.
IT Shop	Specifies whether the system role can be requested through the IT Shop. This system role can be requested by staff through the Web Portal and granted through a defined approval process. The system role can still be assigned directly to employees and hierarchical roles. For more information about IT Shop, see the <i>One Identity Manager IT Shop Administration Guide</i> .
Only for use in IT Shop	Specifies whether the system role can only be requested through the IT Shop. This system role can be requested by staff through the Web Portal and granted through a defined approval process. The system role may not be assigned directly to hierarchical roles.
Spare field no. 01 ... Spare field no. 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.


Related topics

- [Disabled system roles](#) on page 11

Creating and editing system role types

System role types identify the type of company resources that the system role is used to grouped together. You can, for example, define system role types for system roles in which you group different target system groups.

To create or edit a system role type

1. In the Manager, select the **Entitlements > Basic configuration data > System role types** category.
2. Select a system role type in the result list. Select the **Change main data** task.
– OR –
Click  in the result list.
3. Enter a name and description for the system role type.
4. Save the changes.

Assigning company resources to system roles

Assign the company resources you want to group together into one package, to the system role. When you assign system roles to employees and workdesks, the company resources are inherited by the employees and workdesks.

NOTE: Company resources where the **Only use in IT Shop** option is set can only be assigned to system roles that also have this option set.

The following table lists the company resources you can assign to system roles.

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

Table 6: 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 systems	Target System Base Module
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 Module
SAP profiles	SAP R/3 User Management module Module
SAP roles	SAP R/3 User Management module Module
SAP parameters	SAP R/3 User Management module Module
Structural profiles	SAP R/3 Structural Profiles Add-on Module
BI analysis authorizations	SAP R/3 Analysis Authorizations Add-on Module
E-Business Suite permissions	Oracle E-Business Suite 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


Company resource	Available in 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
OneLogin roles	OneLogin Module

To add company resources to a system role

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system 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.

Related topics

- [Assigning system roles](#) on page 24

Assigning system roles to workdesks and employees

You can assign system roles directly or indirectly to employees or workdesks. In the case of indirect assignment, employees (workdesks) and system roles are grouped into hierarchical roles. The number of system roles is calculated from the position in the hierarchy and the direction of inheritance assigned to an employee (or workdesk).

Add employees to a shop as customers so that system roles can be assigned through IT Shop requests. All system roles assigned as product to this shop can be requested by the customers. Requested system roles are assigned to the employees after approval is granted.

NOTE: If the system role is disabled or if the share date is still in the future, the company resources are not inherited.

Prerequisites for indirect assignment to employees

- Assignment of employees and system roles is permitted for role classes (departments, cost centers, locations, or business roles).

Prerequisite for indirect assignment to workdesks

- Assignment of workdesks and system roles is permitted for role classes (departments, cost centers, locations, or business roles).

To configure assignments to roles of a role class

1. In the Manager, select role classes in the **Organizations > Basic configuration data > Role classes** category.
- OR -
In the Manager, select role classes in the **Business roles > Basic configuration data > Role classes** category.
2. Select the **Configure role assignments** task and configure the permitted assignments.
 - To generally allow an assignment, enable the **Assignments allowed** column.
 - To allow direct assignment, enable the **Direct assignments permitted** column.
3. Save the changes.

NOTE: There are other configuration settings that play a role when company resources are inherited through departments, cost centers, locations, and business roles. For example, role inheritance might be blocked or inheritance of employees not allowed. For more detailed information about the basic principles for assigning company resources, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- [Assigning system roles to departments, cost centers, and locations](#) on page 19
- [Assigning system roles to business roles](#) on page 19
- [Adding system roles to the IT Shop](#) on page 20
- [Assigning system roles directly to employees](#) on page 21
- [Assigning system roles directly to workdesks](#) on page 22
- [Adding system roles to system roles](#) on page 23
- [Assigning company resources to system roles](#) on page 15
- [Details of system role inheritance](#) on page 8

Assigning system roles to departments, cost centers, and locations


Assign the system role to departments, cost centers, and locations for it to be assigned to employees and workdesks through these organizations.

To assign a system role to departments, cost centers, and locations

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **Assign organizations** task.
4. In the **Add assignments** pane, assign the organizations:
 - On the **Departments** tab, assign departments.
 - On the **Locations** tab, assign locations.
 - On the **Cost centers** tab, assign cost centers.

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

To remove an assignment

- Select the organization and double-click .
5. Save the changes.

NOTE: In order for company resources assigned to the system role to be inherited by departments, cost centers, and locations, role classes must have the **Direct assignments allowed** option set. For more information about setting this option, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

- [Assigning system roles to business roles](#) on page 19
- [Adding system roles to the IT Shop](#) on page 20
- [Assigning system roles directly to employees](#) on page 21
- [Assigning system roles directly to workdesks](#) on page 22

Assigning system roles to business roles

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


Assign the system role to business roles so that the system role can be assigned to employees and workdesks through business roles.

To assign a system role to business roles

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **Assign business roles** 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.

NOTE: In order for company resources assigned to the system role to be inherited by business roles, role classes must have the **Direct assignments allowed** option set. For more information about setting this option, see the *One Identity Manager Business Roles Administration Guide*.

Related topics

- [Assigning system roles to departments, cost centers, and locations](#) on page 19
- [Adding system roles to the IT Shop](#) on page 20
- [Assigning system roles directly to employees](#) on page 21
- [Assigning system roles directly to workdesks](#) on page 22

Adding system roles to the IT Shop

A system role can be requested by shop customers when it is assigned to an IT Shop shelf. There are other prerequisites to take into account so that a system role can be requested.

- The system role have the **IT Shop** option set.
- The system role must be assigned to a service item.
- If the system role can only be assigned to employees using IT Shop requests, the system role must be also labeled with **Only use in IT Shop**. Then, the system role may no longer be assigned directly to hierarchical roles.

To add a system role to the IT Shop

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select **Add to IT Shop**.
4. In the **Add assignments** pane, assign the system role to IT Shop shelves.
5. Save the changes.

To remove a system role from individual IT Shop shelves

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the system role from the IT Shop shelves.
5. Save the changes.

To remove a system role from all IT Shop shelves

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

The system role is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this system role are canceled in the process.

For more information about the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- [General main data of system roles](#) on page 12
- [Assigning system roles to departments, cost centers, and locations](#) on page 19
- [Assigning system roles to business roles](#) on page 19
- [Assigning system roles directly to employees](#) on page 21
- [Assigning system roles directly to workdesks](#) on page 22

Assigning system roles directly to employees

System roles can be assigned directly or indirectly to employees. Indirect assignment is carried out by allocating the employee and system roles in company structures, like departments, cost centers, locations, or business roles.

To react quickly to special requests, you can assign system roles directly to employees. The employees obtain all company resources assigned to the system role.


NOTE: If the system role is disabled or if the share date is still in the future, the company resources are not inherited.

To assign a system role directly to employees

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **Assign to employees** task.
4. In the **Add assignments** pane, add employees.

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

To remove an assignment

- Select the employee and double-click .
5. Save the changes.

Related topics

- [Assigning system roles to departments, cost centers, and locations](#) on page 19
- [Assigning system roles to business roles](#) on page 19
- [Adding system roles to the IT Shop](#) on page 20
- [Assigning system roles directly to workdesks](#) on page 22

Assigning system roles directly to workdesks

System roles can be assigned directly or indirectly to a contact. Indirect assignment is carried out by allocating the workdesk and system roles in company structures, like departments, cost centers, locations, or business roles.

To react quickly to special requests, you can assign system roles directly to workdesks. The workdesks obtain all company resources assigned to the system role.

NOTE: The company resources are not inherited if the system role is disabled or if the share date is still in the future.

To assign a system role directly to workdesks

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **Assign workdesks** task.
4. In the **Add assignments** pane, assign workdesks.

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

To remove an assignment

- Select the workdesk and double-click ✓.

5. Save the changes.

Related topics

- [Assigning system roles to departments, cost centers, and locations](#) on page 19
- [Assigning system roles to business roles](#) on page 19
- [Adding system roles to the IT Shop](#) on page 20
- [Assigning system roles directly to employees](#) on page 21

Adding system roles to system roles

Use this task to group different system roles into one package. This enables system roles to be structured from different view points.

NOTE: System roles with the **Only use in IT Shop** option set can only be assigned to system roles that also have this option set.

To assign a system role to system roles

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **Assign system roles** task.
4. To assign parent system roles, select the **System Role contained in** tab.

- In the **Add assignments** pane, assign system roles.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click ✓.

5. To assign child system roles, select the **System Role contains** tab.

- In the **Add assignments** pane, assign system roles.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click ✓.

6. Save the changes.

Assigning system roles

By assigning system roles to other system roles, the system roles become structured hierarchically. A system role can be a child and a parent to any other system role.

In the inheritance calculation, child system roles are not treated as assigned company resources. The assignment of system roles to system roles is only used to build a hierarchy.

To structure system roles hierarchically

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **Assign system roles** task.
4. Select the **System role contains** tab.
5. In the **Add assignments** pane, assign the system roles that you want to be children to the selected system role.

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

To remove an assignment

- Select the system role and double-click ✓.
6. Select the **System role contained in** tab.
 7. In the **Add assignments** pane, assign the system roles that you want to be parents to the selected system role.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click ✓.
8. Save the changes.

Related topics

- [Assigning company resources to system roles](#) on page 15

Excluding system roles


Specify, which system role of a pair of system roles, should be take effect if both are assigned. No company resources are inherited by the system role which is not effective.

To exclude system roles

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **Edit conflicting system roles** task.
4. In the **Add assignments** pane, assign system roles that are mutually exclusive to the selected system role.

TIP: In the **Remove assignments** pane, you can remove the system role assignment.

To remove an assignment

- Select the system role and double-click .
5. Save the changes.

Detailed information about this topic

- [Effectiveness of system roles](#) on page 9

Assigning extended properties to system 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.

To specify extended properties for a system role

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system 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.

For more information about extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Displaying the system role overview

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

To obtain an overview of a system role

1. In the Manager, select the **Entitlements > System roles** category.
2. Select the system role in the result list.
3. Select the **System role overview** task.

Configuration parameters for system roles

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

Table 7: Configuration parameters for the module

Configuration parameter	Description
QER ESet	<p>Preprocessor relevant configuration parameter for controlling the database model components for system roles. If this parameter is set, system components are available. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not 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 <i>One Identity Manager Configuration Guide</i>.</p>
QER Structures Inherit ESetExclusion	<p>Preprocessor-relevant configuration parameter for defining the effectiveness of system roles. If this parameter is set, mutually excluding system roles can be defined. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not 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 <i>One Identity Manager Configuration Guide</i>.</p>
QER Structures Inherit NoESetSplitting	<p>Specifies whether the components of a system role are already split in the hierarchical role (as previously) or not (current behavior). If this parameter is set, the system roles are not broken down into their individual components until the target of the inheritance.</p> <p>The configuration parameter does not affect child system roles.</p>

Examples of system role inheritance

The following example shows how inheritance of company resources through system roles works and what effect exclusion definitions have.

Example of a system role hierarchy

The following tables show how assignments to system roles and the system role hierarchy is mapped in the One Identity Manager database.

Table 8: System roles: assignments (ESetHasEntitlement)

System role (UID_ESet)	Assignment System Role (Entitlement)	Origin (XOrigin)
System role A	System role A1	1
System role A	System role A2	1
System role A	System role A11	2
System role A	System role A12	2
System role A1	System role A11	1
System role A1	System role A12	1
System role A1	System entitlement	1
System role A2	Software	1
System role A11	Active Directory group	1
System role A12	SAP role	1
System role B	Resource	1

Table 9: System role hierarchy (table ESetCollection)

System role (UID_ESet)	Child System Role (UID_ESetChild)
System role A	System role A
System role A	System role A1
System role A	System role A2
System role A	System role A11
System role A	System role A12
System role A1	System role A1
System role A1	System role A11
System role A1	System role A12
System role A11	System role A11
System role A12	System role A12
System role A2	System role A2
System role B	System role B

Examples of inheritance paths for system roles

Figure 2: Inheriting an Active Directory group through a directly assigned system role

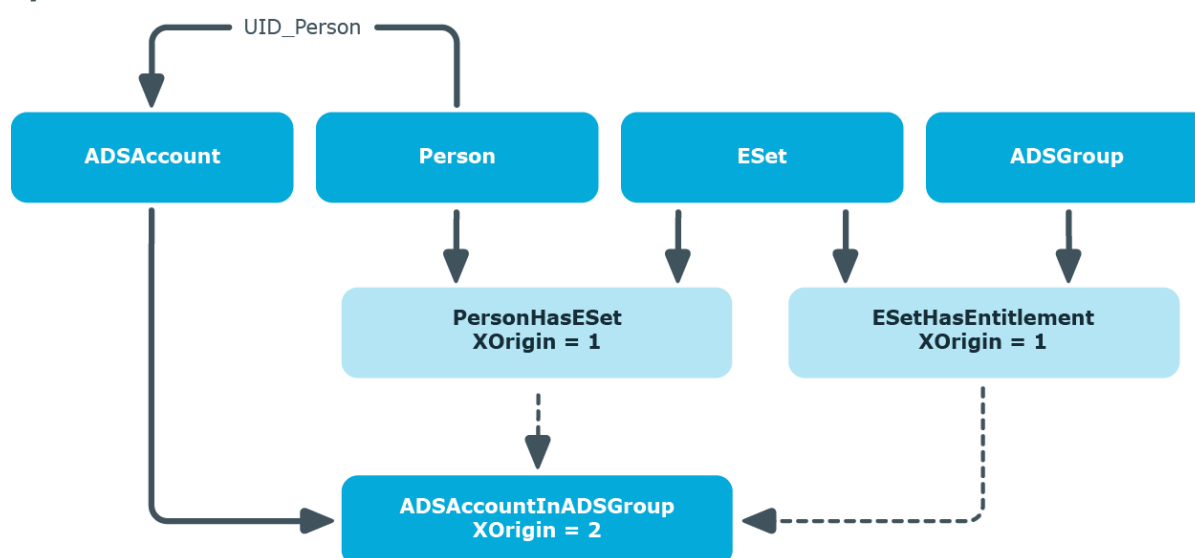


Figure 3: Inheriting software through an IT Shop request

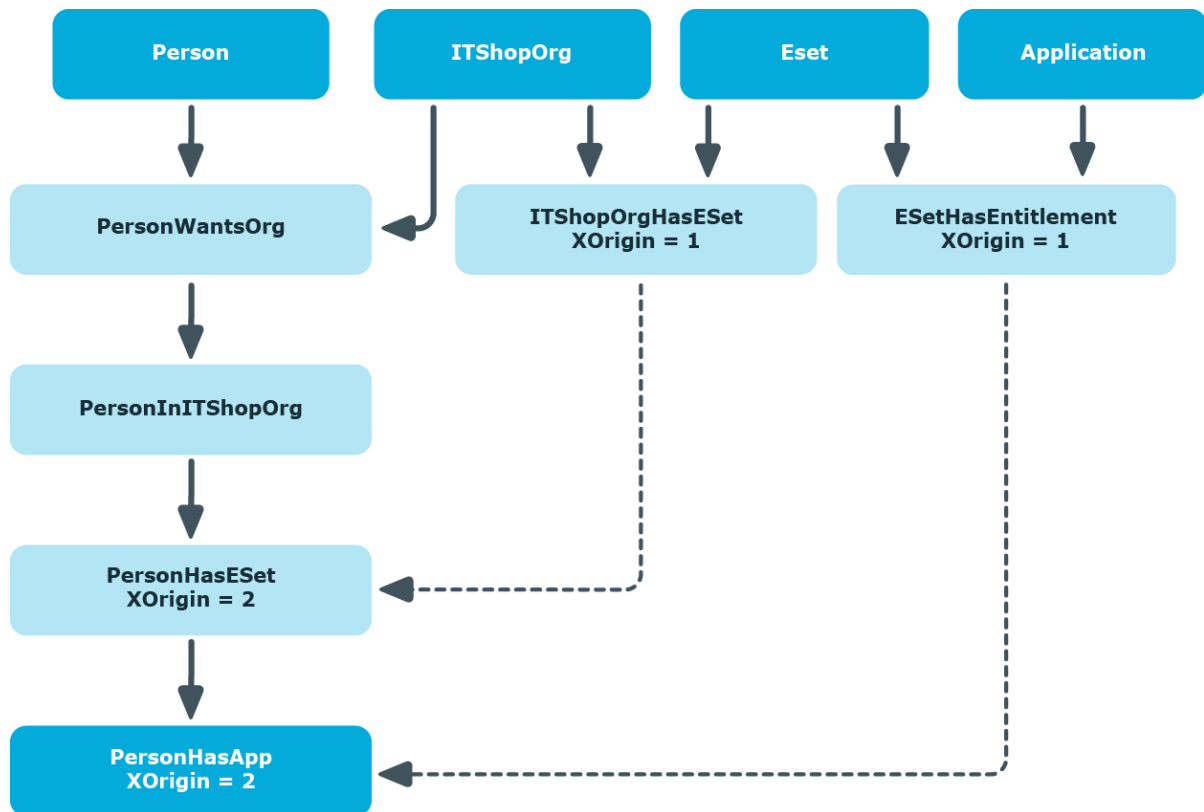
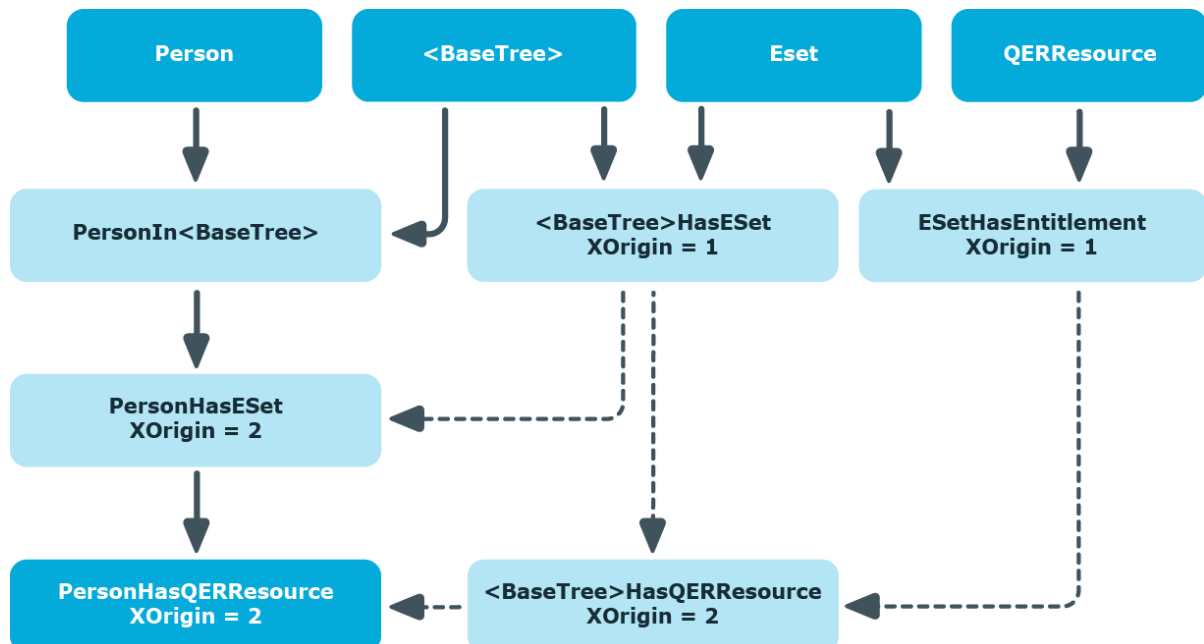


Figure 4: Inheriting a resource through an indirectly assigned system role



Effect of exclusion definitions for system roles

The following images show how excluding a system role affects how inheritance is calculated. Excluded system roles can still be assigned to employees. An option on the column `XIsInEffect` defines whether this assignment applies. Assigning an excluded system role leads to the entry `XIsInEffect = 0`, if the other system role from the exclusion definition is assigned at the same time.

Table 10: Excluded system roles (table `ESetExcludesESet`)

System role (UID_ESet)	Excluded System Role (UID_ESetExcluded)
System role A12	System role A11
System role B	System role B1
System role B	System role A2

Table 11: System roles: inheritance (table `ESetHasEntitlement`)

System role (UID_ESet)	Assignment System Role (Entitlement)	Assignment Applies (XIsInEffect)
System role A	System role A1	1
System role A	System role A2	1
System role A	System role A11	0
System role A	System role A12	1
System role A1	System role A11	0
System role A1	System role A12	1
System role A2	Software	1
System role A11	Active Directory group	1
System role A12	SAP role	1
System role B	Resource R1	1
System role B1	Resource R2	1

```

graph TD
    ADSSAccount --> SAPUser
    ADSSAccount --> Person
    Person --> SAPUser
    Person --> SAPRole
    Person --> ESet_A12
    Person --> ESet_A11
    Person --> ADSSGroup
    SAPRole --> ESetHasEntitlement_A12
    ESet_A12 --> ESetHasEntitlement_A12
    ESet_A12 --> ESetExcludesESet
    ESet_A11 --> ESetExcludesESet
    ESet_A11 --> ESetHasEntitlement_A11
    ADSSGroup --> ESetHasEntitlement_A11
    ESetHasEntitlement_A12 --> PersonHasESet_A12
    ESetExcludesESet --> PersonHasESet_A12
    ESetHasEntitlement_A11 --> PersonHasESet_A11
    ESetHasEntitlement_A11 --> AND1(( ))
    ESetHasEntitlement_A11 --> AND2(( ))
    AND1 --> PersonHasESet_A11
    AND2 --> PersonHasESet_A11
    PersonHasESet_A12 --> SAPUserInSAPRole
    PersonHasESet_A11 --> SAPUserInSAPRole
    SAPUserInSAPRole --> SAPUser
  
```

The flowchart illustrates the execution of a query plan. It starts with a top-level flow that branches into two main paths. The left path involves a **Person** entity leading to **PersonWantsOrg**, then **PersonInITShopOrg**, and finally **PersonHasESet** (XIsInEffect = 1). The right path involves an **ITShopOrg** entity leading to **PersonWantsOrg**, then **PersonInITShopOrg**, and finally **PersonHasESet** (XIsInEffect = 0). In the center, there are two **ESet** entities: **System role B** and **System role A2**. These lead to **ESetHasEntitlement** and **ESetExcludesESet** conditions. These conditions then lead to **ITShopOrgHasESet** (XIsInEffect = 1) and **ITShopOrgHasESet** (XIsInEffect = 1) respectively. These two **ITShopOrgHasESet** entities are connected by a dashed line with a double bar, indicating a logical AND or a specific relationship. Finally, the **ITShopOrgHasESet** (XIsInEffect = 1) entity leads to **PersonHasESet** (XIsInEffect = 1), which then leads to the final result **PersonHasQERResource** (XIsInEffect = 1). The **PersonHasESet** (XIsInEffect = 0) entity also leads to the final result **PersonHasQERResource** (XIsInEffect = 1).

Special features of inheritance system roles through hierarchical roles

Table 12: Configuration parameters for calculating assignments to hierarchical roles

Configuration parameter	Effect when set
QER Structures Inherit NoESetSplitting	Specifies whether or not the components of a system role are already split in the hierarchical role. If this parameter is set, the system roles are not broken down into their individual components until the target of the inheritance.

If this configuration parameter is set, system roles that are assigned to hierarchical roles are not split in the calculation of inheritance. This means that the assignments of company resources to hierarchical roles are not written to the corresponding assignment tables (<BaseTree>Has...). The system roles whose assignments are in effect (PersonHasESet.XIsInEffect = 1) are not split until the calculation of user inheritance.

NOTE: A system role hierarchy is always split. This means the assignment of child system roles to hierarchical roles is always written in the assignment tables. This behavior is independent of the configuration parameter setting.

This configuration parameter is set by default.

Figure 7: Inheritance by indirectly assigned system roles when the configuration parameter is set

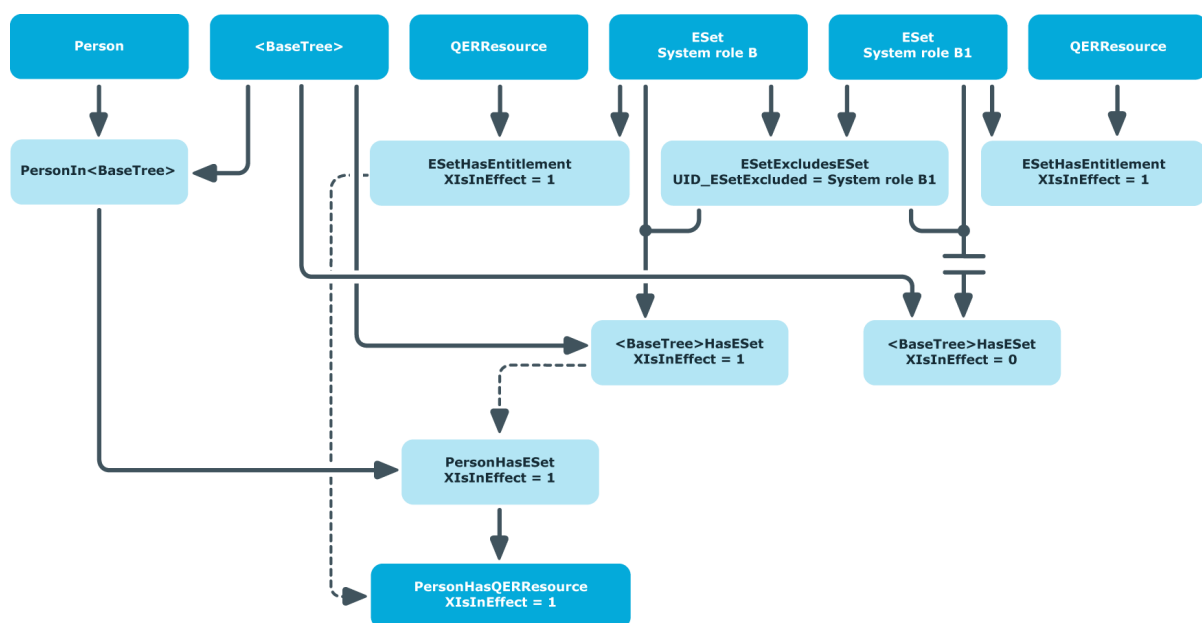
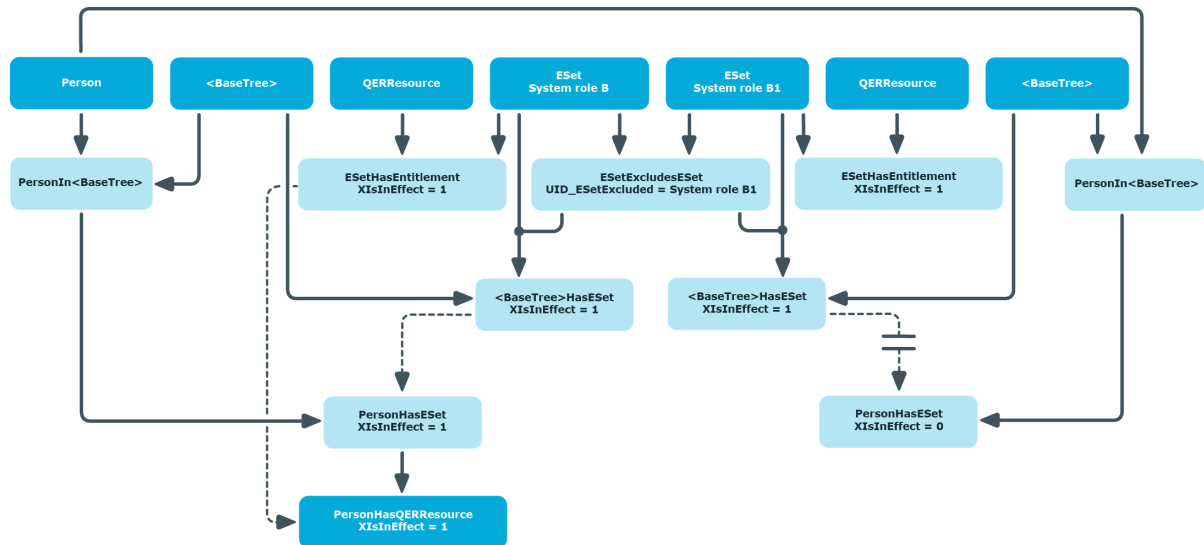
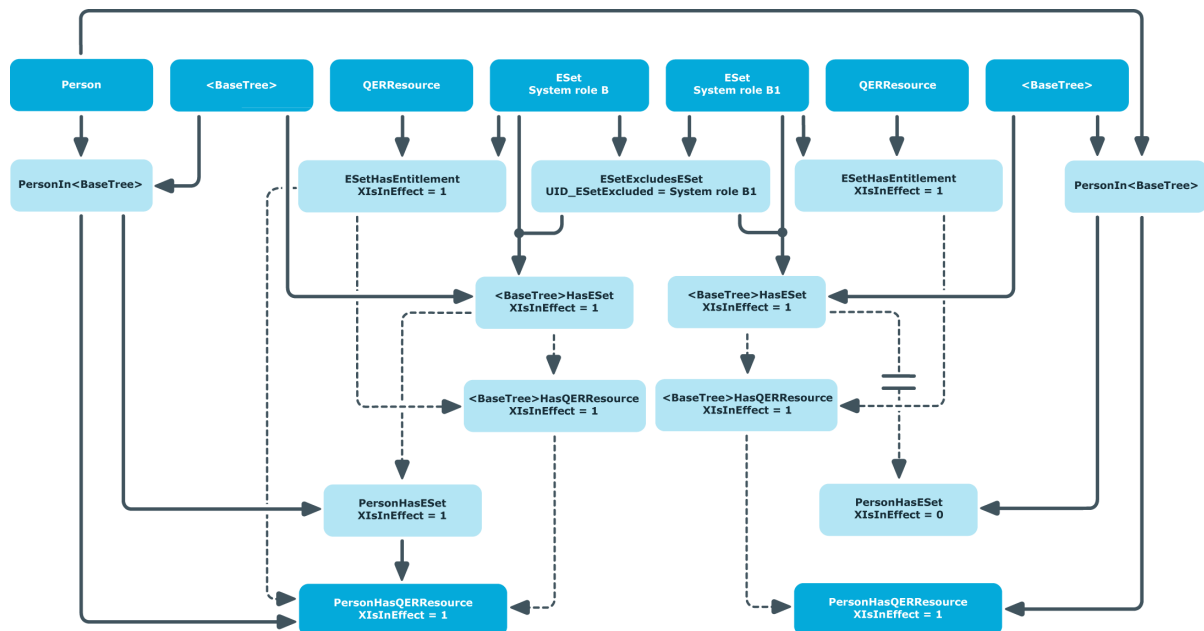


Figure 8: Inheritance by different hierarchical roles when the configuration parameter is set



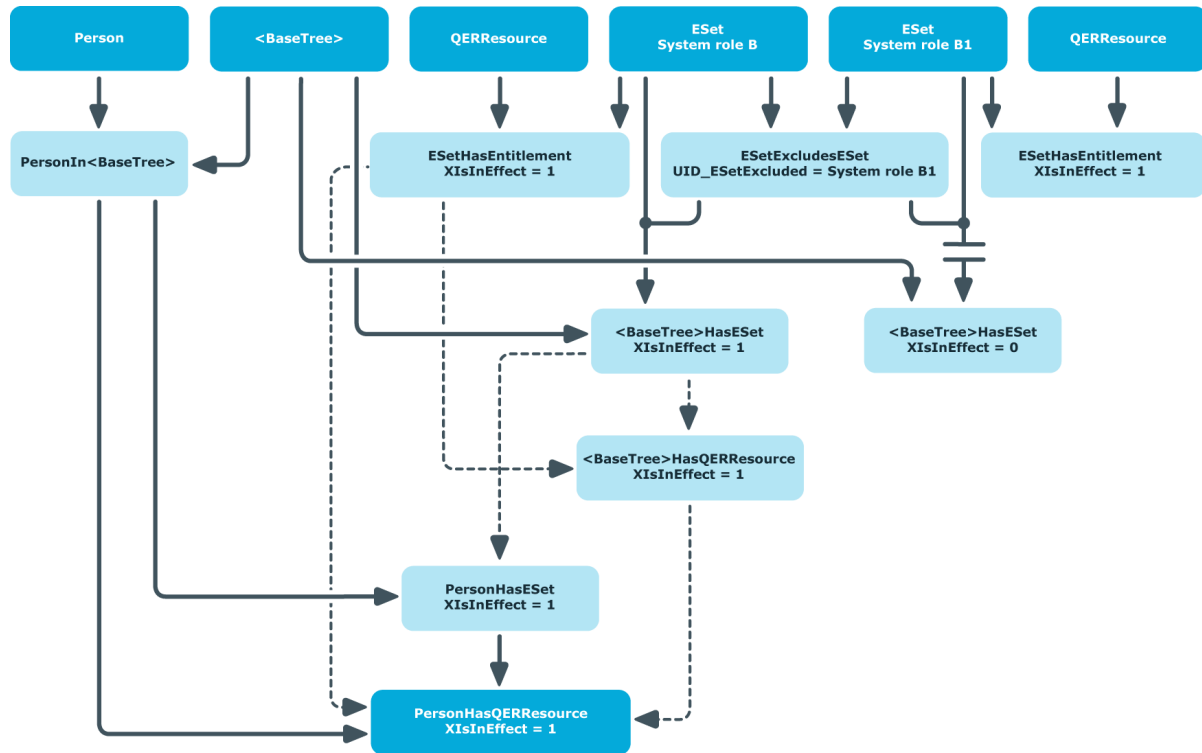
If the configuration parameter is not set, the system roles whose assignments are in effect (BaseTreeHasESet.XIsIneffect = 1) are split in the inheritance calculation for the hierarchical roles. If the excluding system roles are assigned to different hierarchical roles, both assignments are effective. This makes the resulting company resource assignments to hierarchical roles also effective. If an employee is a member of both hierarchical roles, the company resources of the excluded system role are inherited by this employee.

Figure 9: Inheritance by different hierarchical roles when the configuration parameter is not set



If the mutually exclusive system roles are assigned to the same hierarchical role, the exclusion definition takes effect when calculating BaseTreeHasESet.

Figure 10: Inheritance through the same hierarchical role when the configuration parameter is not set



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

Contacting us

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

Technical support resources

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

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

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

A

assign employee 21
assign to workdesk 22

B

business role 19

C

company resource 15
 pass down 7, 11, 29
cost center 19

D

deactivate 12
department 19

E

edit 12
effective business role 9, 24, 31, 33
enable 12
excluded system role 9, 31, 33
exclusion definition 9, 31
extended property 25

I

inheritance 7
 about IT Shop 29, 31
 calculate 29, 31
 direct 29, 31

disabled system role 11
indirect 29, 31, 33
resolve system role 33

IT Shop 12, 20

L

location 19

M

manager 12

S

service item 12
share 12
share date 12
system role 5
 add to system role 23
 exclusion 9, 24
 solve 33
system role hierarchy 7, 24, 28
system role type 12, 15