

Dell™ One Identity Manager 7.1.3

System Roles Administration Guide



© 2016 Dell Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. Dell™, the Dell logo, and Dell™ One Identity Manager, Active Roles, Dell™ One Identity Password Manager, and Dell™ One Identity Cloud Access Manager are trademarks of Dell Inc. in the United States and/or other jurisdictions. Microsoft, Outlook, Active Directory, Azure, SharePoint, SQL Server, Forefront, Internet Explorer, Visual Studio, Windows Server, Windows PowerShell, Windows Vista and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. SAP, SAP R/3, SAP NetWeaver Application Server, SAP HANA, and BAPI are trademarks or registered trademarks of SAP AG (or an SAP affiliate company) in Germany and other countries. IBM, DB2, RACF, Notes, Domino and LotusScript are registered trademarks of International Business Machines Corporation. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Oracle, MySQL and Java are trademarks or registered trademarks of Oracle and/or its affiliates. UNIX is a registered trademark of The Open Group. Mono is a registered trademark of Novell, Inc. Apache and Apache HTTP Server are trademarks of The Apache Software Foundation. Firefox is a registered trademark of the Mozilla Foundation. Safari is a registered trademark of Apple Inc. Chrome and Google are trademarks or registered trademarks of Google Inc., used with permission. CA ACF2 and CA Top Secret are trademarks or registered trademarks of CA Technologies Inc. All other marks and names mentioned herein may be trademarks of their respective companies.

Legend

-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

One Identity Manager System Roles Administration Guide
Updated - November 2017
Version - 7.1.3

Contents

Managing System Roles	4
One Identity Manager Users for Managing System Roles	4
Effectiveness of System Roles	5
System Role Types	7
Editing System Roles	8
Assigning System Roles to Company Resources	9
Assigning System Roles to Workdesks and Employees	11
Assigning System Roles to Departments, Cost Centers and Locations	11
Assigning System Roles to Business Roles	12
Adding System Roles to the IT Shop	13
Assigning System Roles directly to Employees	14
Assigning System Roles directly to Workdesks	14
Adding System Roles to System Roles	15
Additional Tasks for Managing System Roles	15
System Role Overview	16
Assigning Extended Properties	16
Excluding System Roles	16
Appendix: Technical Details about Inheriting Applications	18
About Dell	20
Contacting Dell	20
Technical support resources	20
Index	21

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 the 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.

One Identity Manager components for managing system roles are available if the configuration parameter "QER/ESet" is set.

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

One Identity Manager Users for Managing System Roles

The following users are used for managing system roles.

Table 1: Users

User	Task
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.

User	Task
One Identity Manager administrators	<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, as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configures schedules as required.

Effectiveness of System Roles

By assigning system roles to employees, workdesks or hierarchical roles and through the associated inheritance of company resources, an employee may obtain company resources which should not be assigned to the same person at the same time 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 configuration parameter "QER\Structures\ExcludeStructures" is set.

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 tables `PersonHasESet`, `BaseTreeHasESet` and `WorkdeskHasESet` through the column `XIsInEffect`.

Example for the Effectiveness of System Roles

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

Clara Harris directly assigns the system role "Marketing". She obtains the system role "Finance" through her membership in a business role, the system "Controlling" through an IT Shop request. Clara Harris 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 pay invoices. That means, the system roles "Finance" and "Marketing" are mutually exclusive. An employee that

checks invoices may not be able to make invoice payments as well. That means, the system roles "Finance" and "Controlling" are mutually exclusive.

Table 2: Specifying Mutually Exclusive System Roles (Table ESetsExcludesESet)

Effective Business Role	Excluded System Role
Marketing	
Finance	Marketing
Controlling	Finance

Table 3: Effective Assignments

Employee	Member in System Role	Effective Business Role
Ben King	Marketing	Marketing
Jan Bloggs	Marketing, finance	Finance
Clara Harris	Marketing, finance, controlling	Controlling
Jenny Basset	Marketing, Controlling	Marketing, Controlling

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

Jenny Basset retains the system roles "Marketing" and "Controlling" 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 system role "Controlling".

Table 4: Excluded System Roles and Effective Assignments

Employee	Member in System Role	Excluded System Role (UID_ESetsExcluded)	Effective Business Role
Jenny Basset	Marketing		Controlling
	Controlling	Finance Marketing	

Related Topics

- [Excluding System Roles on page 16](#)

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 edit a system role type

1. Select the category **Entitlements | Basic configuration data | System role types**.
2. Select the system role type in the result list. Select **Change master data** in the task view.
- OR -
Click  in the result list toolbar.
3. Enter a name and description for the system role type.
4. Save the changes.

Editing System Roles

To edit system roles

1. Select the category **Entitlements | System Roles**.
2. Select the resource in the result list. Select **Change master data** in the task view.
- OR -
Click  in the result list toolbar.
3. Edit the system role's master data.
4. Save the changes.

Enter the following data for a system role.

Table 5: System Role Master Data

Property	Description
Display name	Name for displaying the system roles in One Identity Manager tools.
System role	Unique identifier for the system role.
Internal product names	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, see the Dell One Identity Manager IT Shop Administration Guide.
System role manager	You can assign any employee to be a manager for the system role. This employee can edit system role master data. They can be used as attestors for system role properties.

Property	Description
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 option Disabled in these cases.</p> <p>NOTE: Configure and set the schedule "Share system roles" in the Designer to check the share date. For more information, see the Dell One Identity Manager Configuration Guide.</p>
Risk index (calculated)	Maximum risk index values for all company resources. This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set. For more information, see the Dell One Identity Manager Risk Assessment Administration Guide.
Comment	Spare text box for additional explanation.
Remarks	Spare text box for additional explanation.
Description	Spare text box for additional explanation.
Disabled	<p>Specifies whether employees inherit the company resources contained in the system role.</p> <p>If the option is set, the system role can be assigned to employees. However they cannot inherit the company resources contained in the system role.</p> <p>If the option is not set, the employees that are assigned the system role, immediately inherit company resources allocated to the system role.</p> <p>If the option is enabled at a later date, existing assignments are removed.</p>
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 the request granted by a defined approval procedure. The system role can still be assigned directly to employees and hierarchical roles. For more information, see the Dell One Identity Manager IT Shop Administration Guide.
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 the request granted by a defined approval procedure. The system role may not assigned directly to hierarchical roles. For more information, see the Dell One Identity Manager IT Shop Administration Guide.
Spare fields no. 01.....spare field no. 10	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Assigning System Roles to Company Resources

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

- ① **NOTE:** Company resources with the option **Only use in IT Shop** can only be assigned to system roles that also have this option set.
- ① **NOTE:** Company resources are defined in the One Identity Manager modules and are not available until the modules are installed.

Table 6: Possible Assignments of Company Resources to System Roles

Company Resource	Available in Module
Resources	always
Account definitions	Target System Base Module
Groups of custom target systems	Target System Base Module
Active Directory® groups	Active Directory Module
SharePoint® groups	SharePoint Module
SharePoint® roles	SharePoint Module
LDAP groups	LDAP Module
Notes groups	IBM Notes Module
SAP groups	SAP R/3 User Management module Module
SAP profiles	SAP R/3 User Management module Module
SAP roles	SAP R/3 User Management module Module
Structural profiles	SAP R/3 Structural Profiles Add-on Module
BI analysis authorizations	SAP R/3 Analysis Authorizations Add-on Module
System Roles	System Roles Module
Subscribable reports	Report Subscription Module
Applications	Application Management Module
Azure® Active Directory® groups	Azure Active Directory Module
Azure® Active Directory® Administrator Roles	Azure Active Directory Module

To add company resources to a system role

1. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select the task to assign the corresponding company resource.
4. Assign company resources in **Add assignments**.
- OR -
Remove company resource in **Remove assignments**.
5. Save the changes.

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).

Prerequisites for indirect assignment to employees

- Assignment of employees and system roles is permitted for role classes (department, cost center, location or business role).

Prerequisites for indirect assignment to workdesks

- Assignment of workdesks and system roles is permitted for role classes (department, cost center, location or business role).

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.

① **NOTE:** The company resources are not inherited if the system role is disabled or if the share date is still in the future.

Detailed information about this topic

- [Assigning System Roles to Departments, Cost Centers and Locations on page 11](#)
- [Assigning System Roles to Business Roles on page 12](#)
- [Adding System Roles to the IT Shop on page 13](#)
- [Assigning System Roles directly to Employees on page 14](#)
- [Assigning System Roles directly to Workdesks on page 14](#)
- [Adding System Roles to System Roles on page 15](#)

Related Topics

- [Assigning System Roles to Company Resources on page 9](#)
- [Appendix: Technical Details about Inheriting Applications on page 18](#)
- [Dell One Identity Manager Identity Management Base Module Administration Guide](#)

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. Select the category **Entitlements | System Roles**.
 2. Select the system role in the result list.
 3. Select **Assign organizations**.
 4. Assign organizations in **Add assignments**.
 - Assign departments on the **Departments** tab.
 - Assign locations on the **Locations** tab.
 - Assign cost centers on the **Cost center** tab.
- OR -
- Remove the organizations from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning System Roles to Business Roles on page 12](#)
- [Adding System Roles to the IT Shop on page 13](#)
- [Assigning System Roles directly to Employees on page 14](#)
- [Assigning System Roles directly to Workdesks on page 14](#)

Assigning System Roles to Business Roles

Installed Modules: Business Roles Module

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. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.
 - OR -
 - Remove business roles from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning System Roles to Departments, Cost Centers and Locations on page 11](#)
- [Adding System Roles to the IT Shop on page 13](#)
- [Assigning System Roles directly to Employees on page 14](#)
- [Assigning System Roles directly to Workdesks on page 14](#)

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

To add a system role to the IT Shop

1. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the system role to IT Shop shelves in **Add assignments**.
5. Save the changes.

To remove a system role from individual IT Shop shelves

1. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the system role from the shelves in **Remove assignmentsIT Shop**.
5. Save the changes.

To remove a system role from all IT Shop shelves

1. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
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.

Detailed information about this topic

- [Dell One Identity Manager IT Shop Administration Guide](#)

Related Topics

- [Editing System Roles](#) on page 8
- [Assigning System Roles to Departments, Cost Centers and Locations](#) on page 11
- [Assigning System Roles to Business Roles](#) on page 12

- [Assigning System Roles directly to Employees on page 14](#)
- [Assigning System Roles directly to Workdesks on page 14](#)

Assigning System Roles directly to Employees

System roles can be assigned directly or indirectly to a 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.

① **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 employees

1. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select **Assign to employees** in the task view.
4. Assign employees in **Add assignments**.
- OR -
Remove employees from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning System Roles to Departments, Cost Centers and Locations on page 11](#)
- [Assigning System Roles to Business Roles on page 12](#)
- [Adding System Roles to the IT Shop on page 13](#)
- [Assigning System Roles directly to Workdesks on page 14](#)

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.

① **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. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.

3. Select **Assign workdesks** in the task view.
4. Assign workdesks in **Add assignments**.
- OR -
Remove workdesks from **Remove assignments**.
5. Save the changes.

Related Topics

- [Assigning System Roles to Departments, Cost Centers and Locations on page 11](#)
- [Assigning System Roles to Business Roles on page 12](#)
- [Adding System Roles to the IT Shop on page 13](#)
- [Assigning System Roles directly to Employees on page 14](#)

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.

- ① **NOTE:** System roles with the option **Only use in IT Shop** set can only be assigned to system roles that also have this option set.

To assign a system role to system roles

1. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select **Assign system roles in the task view**.
4. Select the tab **System role contained in** to assign parent system roles.
 - Assign system roles in **Add assignments**.
 - OR -
Remove assignments to system roles in **Remove assignments**.
5. Select the tab **System role contains** to assign child system roles.
 - Assign system roles in **Add assignments**.
 - OR -
Remove assignments to system roles in **Remove assignments**.
6. Save the changes.

Additional Tasks for Managing System Roles

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

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. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select **System role overview** in the task view.

Assigning Extended Properties

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

To specify extended properties for a system role

1. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.
The view- OR -
Remove extended properties from **Remove assignments**.
5. Save the changes.

Detailed information about this topic

- Dell One Identity Manager Identity Management Base Module Administration Guide

Excluding System Roles

Table 7: Configuration Parameters for Editing Mutually Exclusive Roles

Configuration parameter	Active Meaning
QER\Structures\ExcludeStructures	Preprocessor relevant configuration parameter for defining the effectiveness of role memberships. If this parameter is set, mutually excluding roles can be defined (AERoleExcludesAERole, DepartmentExcludesDepartment, LocalityExcludesLocality, OrgExcludesOrg, ProfitCenterExcludesProf, ESetExcludesESet). Changes to the parameter require recompiling the database.

By assigning system roles to employees, workdesks or hierarchical roles and through the associated inheritance of company resources, an employee may obtain company resources which should not be assigned to the same person at the same time 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 configuration parameter "QER\Structures\ExcludeStructures" is set.

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.

To exclude system roles

1. Select the category **Entitlements | System Roles**.
2. Select the system role in the result list.
3. Select **Edit conflicting system roles** in the task view.
4. Assign the system roles that are mutually exclusive to the selected system role in **Add assignments**.
- OR -
Remove the system roles that no longer mutually exclusive in **Remove assignments**.
5. Save the changes.

Detailed information about this topic

- [Effectiveness of System Roles](#) on page 5

Appendix: Technical Details about Inheriting Applications

Assignments of company resources to system roles are mapped in the `ESetHasEntitlement` table. Assignments of system roles to roles are mapped in the `<BaseTree>HasESet` tables.

Employees can directly obtain system roles. Employees also inherit all the system roles belonging to all roles of which they are members (table `PersonIn<Basetree>`) as well as system roles of all roles that are referenced through foreign key relations (table `Person`, column `UID_<BaseTree>`). Direct and indirect assignments of system roles to employees are mapped in the table `PersonHasESet`.

A workdesk can obtain system roles directly. Workdesks also inherit all the system roles belonging to all roles of which they are members (table `WorkDeskIn<Basetree>`) as well as system roles of all roles that are referenced through foreign key relations (table `Workdesk`, column `UID_<BaseTree>`). Direct and indirect assignments of system roles to workdesks are mapped in the table `WorkdeskhasESet`.

System roles are resolved by inheritance. Their components become members of the company resource union set `Prerequisite` is that each company resource can really be inherited.

Example

A system role contain an Active Directory® group and an SAP role. An employee only owns an Active Directory® user account (table `ADSAccount`, column `UID_Person`). If the system role is assigned to the employee (table `PersonHasESet`), the Active Directory® group is inherited by the Active Directory® user account (table `ADSAccountInADSGroup`). The SAP role is not inherited. If this employee obtains an SAP user account (table `SAPUser`, column `UID_Person`) at a later date, the SAP role is inherited by the SAP user account (table `SAPUserInSAPGroup`).

Figure 1: Example of direct assignment of system roles to employees

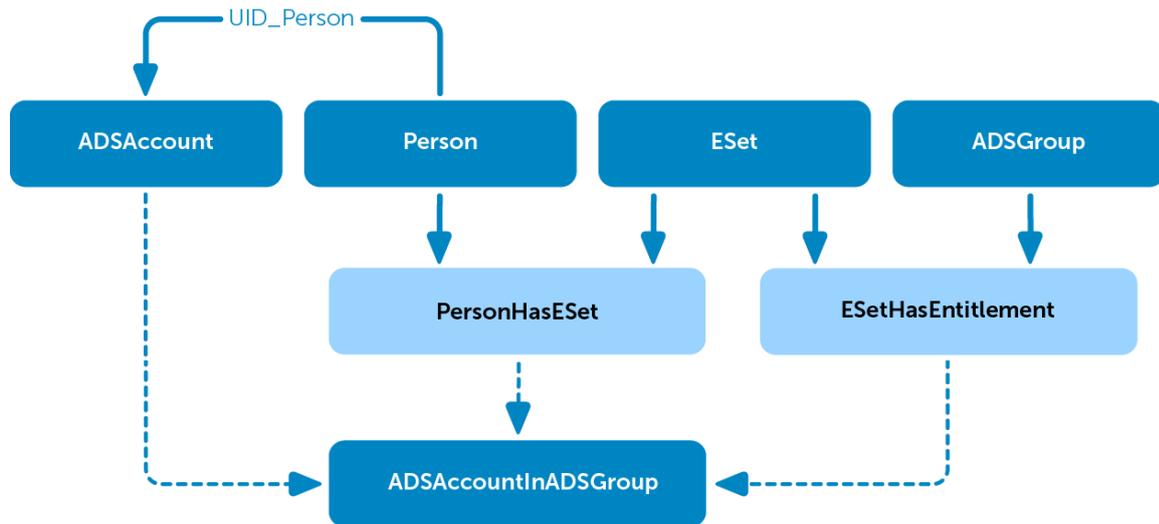
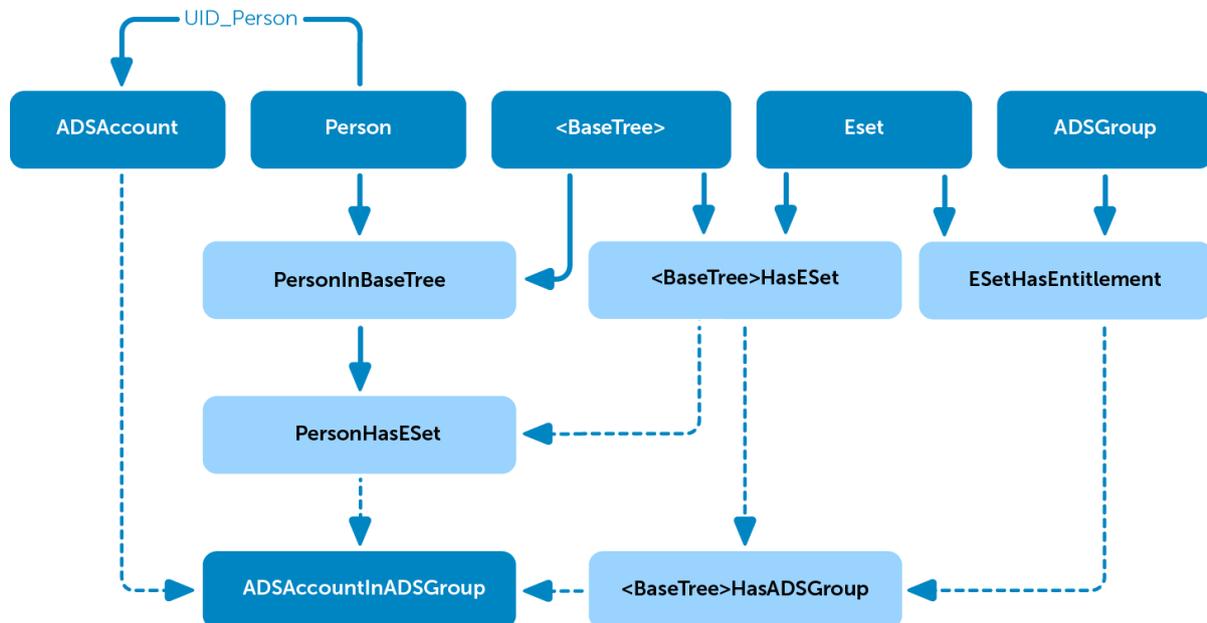


Figure 2: Example of indirect assignment of system roles to employees



Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.quest.com.

Contacting Dell

For sales or other inquiries, visit <http://quest.com/company/contact-us.aspx> or call +1 949 754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to <https://support.quest.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. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to <http://quest.com/trials>.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer

S

- service item 8
- share 8
- share date 8
- system role 4
 - add to system role 15
 - assign to employee 11
 - assign to workdesk 11
- system role type 7-8

A

- assign employee 14
- assign to workdesk 14

B

- business role 12

C

- company resource 9
- cost center 11

D

- department 11

E

- edit 8
- effective business role 16
- exclude system role 16
- exclusion definition 16
- extended property 16

I

- inheritance 11
- IT Shop 8, 13

L

- location 11

M

- manager 8