One Identity Manager 9.1.3

Administration Guide for Connecting to Custom Target Systems

Copyright 2024 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/trademark-information.aspx. 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 Administration Guide for Connecting to Custom Target Systems
Updated - 29 April 2024, 14:22

For the most recent documents and product information, see Online product documentation.

Contents

Managing custom target systems **7**
One Identity Manager users for managing custom target systems 8
Configuration parameters for managing custom target systems 10

Setting up scripted data provisioning in a custom target system **11**
Creating the scripts for data provisioning in a custom target system 12
Job server for provisioning data in a custom target system 13
General main data of Job servers 13
Specifying server functions 16
Post-processing outstanding objects 17
Adding custom tables to the target system synchronization 18
Post-processing outstanding objects 19

Managing user accounts and employees **21**
Account definitions for user accounts 22
Creating account definitions 23
Editing account definitions 23
Main data for account definitions 24
Editing manage levels 26
Creating manage levels 27
Assigning manage levels to account definitions 28
Main data for manage levels 29
Creating mapping rules for IT operating data 30
Entering IT operating data 31
Modify IT operating data 32
Assigning account definitions to employees 33
Assigning account definitions to departments, cost centers, and locations 34
Assigning account definitions to business roles 35
Assigning account definitions to all employees 36
Assigning account definitions directly to employees 36
Assigning account definitions to system roles 37
Adding account definitions in the IT Shop 37
Assigning account definitions to custom target systems 40

Deleting account definitions ... 40
Assigning employees automatically to user accounts ... 43
Editing search criteria for automatic employee assignment ... 45
Finding employees and directly assigning them to user accounts ... 46
Changing manage levels for user accounts ... 47
Assigning account definitions to linked user accounts ... 48
Supported user account types ... 48
Default user accounts ... 50
Administrative user accounts ... 51
Providing administrative user accounts for one employee ... 51
Providing administrative user accounts for several employees ... 52
Privileged user accounts ... 53
Setting deferred deletion for custom target system user accounts ... 54

Managing assignments of groups and system entitlements ... 57
Specifying types of system entitlements in use ... 57
Assigning groups and system entitlements to user accounts in One Identity Manager ... 60
Prerequisites for indirect assignments of groups and system entitlements to user accounts ... 61
Assigning groups to departments, cost centers, and locations ... 62
Assigning system entitlements to departments, cost centers, and locations ... 64
Assigning groups to business roles ... 65
Assigning system entitlements to business roles ... 66
Adding groups to system roles ... 68
Adding system entitlements to system roles ... 68
Adding groups to the IT Shop ... 70
Adding system entitlements to the IT Shop ... 71
Assigning user accounts directly to a group ... 74
Assigning user accounts directly to a system entitlement ... 75
Assigning groups directly to user accounts ... 76
Assigning system entitlements directly to a user account ... 77
Effectiveness of memberships in groups and system entitlements ... 78
Inheriting groups and system entitlements based on categories ... 81
Overview of all assignments ... 83

Login information for user accounts ... 85
Password policies for user accounts ... 85

Predefined password policies ... 86
Using password policies ... 87
Editing password policies ... 88
Creating password policies ... 89
General main data of password policies ... 89
Policy settings ... 90
Character classes for passwords ... 91
Custom scripts for password requirements ... 93
Checking passwords with a script ... 93
Generating passwords with a script ... 94
Editing the password excluded list ... 96
Verifying passwords ... 96
Testing password generation ... 96
Initial password for new user accounts ... 97
Email notifications about login data ... 97

Mapping custom target system objects in One Identity Manager ... 99
Custom target system identifiers ... 99
General main data for custom target systems ... 100
Customizing data synchronization for custom target systems ... 103
Defining categories for inheriting groups and system entitlements ... 103
Specifying alternative column names ... 104
Container structures in custom target systems ... 105
Main data for containers ... 105
User accounts in custom target systems ... 106
Creating and editing user accounts ... 106
User account main data ... 107
Assigning extended properties to user accounts ... 111
Assigning permissions controls to user accounts ... 112
Disabling user accounts ... 112
Deleting and restoring user accounts ... 114
Displaying the user account overview ... 115
Groups in custom target systems ... 115
Main data for groups ... 116
Assigning groups to groups ... 117
Assigning extended properties to groups ... 118

Assigning permissions controls to groups ... 118
Displaying the group overview ... 119
System entitlements in custom target systems ... 119
System entitlement main data ... 120
Assigning system entitlements to system entitlements ... 122
Assigning extended properties to system entitlements ... 123
Displaying system entitlement overviews ... 124
Permissions controls in custom target systems ... 124
Main data for permissions controls ... 125
Assigning user accounts to permissions controls ... 125
Assigning groups to permissions controls ... 126
Displaying the permissions control overview ... 127
Reports about custom target systems ... 127

Treatment of custom target system objects in the Web Portal ... 130

Basic configuration data for custom target systems ... 132
Target system managers ... 133
Target system types for custom target systems ... 136
Configuring display of custom schema extensions for custom target systems ... 137

Appendix: Configuration parameters for managing custom target systems 140

About us ... 142
Contacting us ... 142
Technical support resources ... 142

Index ... 143

Managing custom target systems

You can also map your own implementations, such as telephone systems, in One Identity Manager along side directly supported target systems. To manage these target systems with One Identity Manager, create container structures, user accounts, groups, and system entitlements. Groups and system entitlements represent the objects used in the target system to control access to target system resources.

NOTE: The Target System Base Module module must be installed as a prerequisite for managing custom target systems in One Identity Manager. For more information about installing, see the *One Identity Manager Installation Guide*.

The One Identity Manager components for managing custom target systems are available if the **TargetSystem | UNS | CreateNewRoot** 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*.

- Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.

Define a custom process to swap data between the target system and the One Identity Manager database. One Identity Manager offers different ways of transferring data.

- One Identity Manager provides predefined processes for data provisioning in the default installation. The processes use scripts for data provisioning. Provisioning data from One Identity Manager into the custom target system must be customized because each custom target system maps the data differently. For more information, see Setting up scripted data provisioning in a custom target system on page 11.
- Alternatively, you can set up scripted synchronization using a CSV connector. This requires a large amount of customizing. For more information about this, see the *One Identity Manager CSV Connector User Guide*.
- The Data Import program gives One Identity Manager a simple means of importing data from other systems. The program supports importing from `.csv` files and

importing directly from other database systems. For more information, see the *One Identity Manager Operational Guide*.

One Identity Manager users for managing custom target systems

The following users are used for setting up and administration of custom target systems.

Table 1: Users

Users	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems | Administrators** application role. Users with this application role: • Administer application roles for individual target system types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles for target system managers are mutually exclusive. • Authorize other employees to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the **Target systems | Custom target systems** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects. • Edit password policies for the target system. • Prepare groups and system entitlements to add to the IT Shop. • Can add employees who have another identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and

Users	Tasks
	One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
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: • 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. • Create and configure password policies as required.
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role: • Assign groups to IT Shop structures. • Assign system entitlements to IT Shop structures.
Administrators for organizations	Administrators must be assigned to the **Identity Management | Organizations | Administrators** application role. Users with this application role: • Assign groups to departments, cost centers, and locations. • Assign system entitlements to departments, cost centers, and locations.
Business roles administrators	Administrators must be assigned to the **Identity Management | Business roles | Administrators** application role. Users with this application role:

Users	Tasks
	• Assign groups to business roles. • Assign system entitlements to business roles.

Configuration parameters for managing custom target systems

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

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

For more information, see Configuration parameters for managing custom target systems on page 140.

2

Setting up scripted data provisioning in a custom target system

One Identity Manager provides predefined processes for data provisioning in the default installation. The processes use scripts for data provisioning. Provisioning data from One Identity Manager into the custom target system must be customized because each custom target system maps the data differently.

Processes are handled by the generic web service. For more detailed information about calling the generic web service, see the *One Identity Manager Configuration Guide*.

To use this provisioning procedure, the following steps are required:

- Creating the provisioning script

  Scripts are used to provision data from the One Identity Manager in a custom target system. These must be created for each target system. For more information, see Creating the scripts for data provisioning in a custom target system on page 12.

- Providing a server for provisioning

  On the server, the One Identity Manager Service must be installed, configured, and started. The server must be declared in One Identity Manager and entered as the synchronization server in the target system. For more information, see Job server for provisioning data in a custom target system on page 13.

- Set up custom target systems in the One Identity Manager database and customize synchronization methods in the One Identity Manager database.

  Select the **Synchronization by script** synchronization method. For more information, see Custom target system identifiers on page 99.

TIP: Alternatively, you can set up scripted synchronization using a CSV connector. This requires a large amount of customizing. For more information about this, see the *One Identity Manager CSV Connector User Guide*.

Creating the scripts for data provisioning in a custom target system

In One Identity Manager, default installation processes for the standard events (Insert, Update, Delete) are made available for tables, which are used for mapping custom target systems.

The processes use scripts for data provisioning. The scripts must be modified to fit the custom target system because each custom target system maps the data differently.

Create custom scripts for your target system. You can use the `TSB_Uns_Generic_Templates` script as a template for creating custom scripts.

The processes expect functions in the script that are named with the following format:

`<customer prefix>_<table>_<Ident_UNSRoot>_<event>`

Example: Entering user accounts in the **Telephone system** custom target system

`CCC_UNSAccountB_Telephonesystem_Insert`

IMPORTANT: If your target system contains a hyphen (-) in its name, you must remove it from the script function in the <**Ident_UNSRoot**> part. Otherwise, error may occur during script processing.

The objects in the custom target system are mapped in the following table schema One Identity Manager table.

Table 2: Tables in the One Identity Manager schema for mapping custom target systems

Table	Description
UNSAccountB	User account mapping.
UNSAccountBHasUNSGroupB	Group assignments to user accounts.
UNSAccountBHasUNSGroupB1, UNSAccountBHasUNSGroupB2, UNSAccountBHasUNSGroupB3	Assignments of system entitlements to user accounts.
UNSAccountBHasUNSItemB	Permissions control assignments to user accounts.
UNSAccountBInUNSGroupB	Assignments of user accounts to groups.
UNSAccountBInUNSGroupB1, UNSAccountBInUNSGroupB2, UNSAccountBInUNSGroupB3	Assignments of user accounts to system entitlements.
UNSContainerB	Container structure mapping.
UNSGroupB	Group mapping.
UNSGroupB1, UNSGroupB2, UNSGroupB3	Mapping of other system entitlements.

Table	Description
UNSGroupBHasUnsItemB	Permissions control assignments to groups.
UNSGroupBInUNSGroupB	Assignments of groups to groups (group hierarchy).
UNSGroupB1InUNSGroupB1, UNSGroupB1InUNSGroupB2, UNSGroupB1InUNSGroupB3	Assignments of system entitlements to system entitlements (system entitlement hierarchy).
UNSItemB	Mapping of additional permissions controls.
UNSRootB	Basis for mapping custom target systems.

Job server for provisioning data in a custom target system

You can define a server for each custom target system, which runs all the One Identity Manager Service actions required for provisioning target system objects. For more information about installing and configuring the One Identity Manager Service, see the *One Identity Manager Installation Guide*.

To set up a server

1. Provide a server installed with the One Identity Manager Service.
2. In the Manager, create an entry for the Job server.
    1. Select the **Custom Target Systems > Basic configuration data > Servers** category.
    2. Click in the result list.
    3. Edit the Job server's main data.
    4. Save the changes.
3. Enter the server as the synchronization server in the custom target system.

Detailed information about this topic

- General main data of Job servers on page 13
- Customizing data synchronization for custom target systems on page 103

General main data of Job servers

NOTE: All editing options are also available in the Designer under **Base Data > Installation > Job server**.

NOTE: More properties may be available depending on which modules are installed.

Table 3: Job server properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Syntax: `<Name of server>.<Fully qualified domain name>`
Target system	Computer account target system.
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The **Server is cluster** and **Server belongs to cluster** properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the `Robocopy` and `rsync` programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the `Robocopy` program between servers with a Windows operating system or with the `rsync` program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the implementing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is

Property	Meaning
	automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the `QBM_PJobQueueLoad` procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
Paused due to unavailability of a target system	Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed. For more information about offline mode, see the *One Identity Manager Target System Synchronization Reference Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update	Specifies whether a software update is currently running.

Property	Meaning
running	
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- Specifying server functions on page 16

Specifying server functions

NOTE: All editing options are also available in the Designer under **Base Data > Installation > Job server**.

NOTE: More server functions may be available depending on which modules are installed.

Table 4: Permitted server functions

Server function	Remark
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are not labeled as domain controllers are considered to be member servers.
Printer server	Server that acts as a print server.
Generic server	Server for generic synchronization with a custom target system.
Home server	Server for adding home directories for user accounts.
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks. The server with the One Identity Manager database installed on it is labeled with this functionality during initial installation of the schema.
SQL processing server	It can run SQL tasks. The server requires a direct connection to the database server that One Identity Manager database is installed on. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	This server can process CSV files using the `ScriptComponent` process component.
Generic database	This server can connect to an ADO.Net database.

Server function	Remark
connector	
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server synchronizes the One Identity Manager target system.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
Primary domain controller	Primary domain controller.
Profile server	Server for setting up profile directories for user accounts.
SAM synchronization Server	Server for synchronizing an SMB-based target system.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Windows PowerShell connector	The server can run Windows PowerShell version 3.0 or later.

Post-processing outstanding objects

Objects from custom target systems can be loaded in to the One Identity Manager database at regular intervals by custom processes. This gives you the option to either delete objects directly in the One Identity Manager database or mark them as outstanding, if they do not exist in the target system. For more information, see the *One Identity Manager Target System Synchronization Reference Guide*.

Objects, which do not exist in the target system, can be marked as outstanding in One Identity Manager by synchronizing. This prevents objects being deleted because of an incorrect data situation or an incorrect synchronization configuration.

Outstanding objects:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronizations.
- Are ignored by inheritance calculations.

This means, all memberships and assignments remain intact until the outstanding objects have been processed.

Start target system synchronization to do this.

To allow post-processing of outstanding objects

- Configure target system synchronization on the target system type of the target system to be synchronized.

Related topics

- Adding custom tables to the target system synchronization on page 18
- Target system types for custom target systems on page 136
- Post-processing outstanding objects on page 19

Adding custom tables to the target system synchronization

To post-process outstanding objects, assign the custom target system's target system type to tables, which can contain outstanding objects. Specify the tables for which outstanding objects can be published in the target system during post-processing.

To add tables to target system synchronization

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Target system types** category.
2. In the result list, select the target system type of the customer target system.
3. Select the **Assign synchronization tables** task.
4. In the pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
8. Save the changes.

To publish outstanding objects

1. Create processes that perform provisioning of objects for:
    - Simple tables
    - Assignment tables that contain additional information, such as a valid-from date

   Use the `AdHocProjection` process task of the `ProjectorComponent` process component.

For more information about defining processes, see the *One Identity Manager Configuration Guide*.

2. Create the `HandleOutstanding` event for these processes.

For memberships mapped to simple assignment tables, the **Dependencies modified on** (`XDateSubItem` column) is changed on the base table of the mapping when publishing. This triggers the default update process that is set up for this base table. For more information about provisioning memberships, see the *One Identity Manager Target System Synchronization Reference Guide*.

For more information, see Setting up scripted data provisioning in a custom target system on page 11.

NOTE: If you use the CSV connector for provisioning, ensure that the CSV connector has write access to the CSV files. That means, the **Connection is read-only** option must not be set for the target system connection. For more information, see the *One Identity Manager Target System Synchronization Reference Guide*.

Post-processing outstanding objects

To post-process outstanding objects

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Target system synchronization: <target system>** category.

   All tables assigned to the target system type are displayed in the navigation view.

2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.

   All objects that are marked as outstanding are shown. The **Last log entry** and **Last method run** columns display the time at which the last entry was made in the synchronization log and which processing method was run. The **No log available** entry can mean the following:

   - The synchronization log has already been deleted.

     - OR -

   - An assignment from a member list has been deleted from the target system.

     The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.

   - An object that contains a member list has been deleted from the target system.

     During synchronization, the object and all corresponding entries in the assignment tables are marked as outstanding. However, an entry in the synchronization log appears only for the deleted object.

   TIP:

To display object properties of an outstanding object

1. Select the object on the target system synchronization form.
2. Open the context menu and click **Show object**.

3. Select the objects you want to rework. Multi-select is possible.
4. Click on one of the following icons in the form toolbar to run the respective method.

Table 5: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The **Outstanding** label is removed from the object. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The **Outstanding** label is removed for the object.

5. Confirm the security prompt with **Yes**.

NOTE: By default, the selected objects are processed in parallel, which speeds up the selected method. If an error occurs during processing, the action is stopped and all changes are discarded.

Bulk processing of objects must be disabled if errors are to be localized, which means the objects are processed sequentially. Failed objects are named in the error message. All changes that were made up until the error occurred are saved.

To disable bulk processing

- Disable the icon in the form's toolbar.

Related topics

- Adding custom tables to the target system synchronization on page 18

3

Managing user accounts and employees

The main feature of One Identity Manager is to map employees together with the main data and permissions available to them in different target systems. To achieve this, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This provides an overview of the permissions for each employee in all of the connected target systems. One Identity Manager offers the option of managing user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

Because requirements vary between companies, One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following methods for linking employees and their user accounts:

- Employees can automatically obtain their account definitions using user account resources.

  If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanisms and subsequent process handling.

  When you manage account definitions through user accounts, you can specify the way user accounts behave when employees are enabled or deleted.
- When user accounts are inserted, they can be automatically assigned to an existing employee or a new employee can be created if necessary. In the process, the employee main data is created on the basis of existing user account main data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. You must define criteria for finding employees for automatic employee assignment.
- Employees and user accounts can be entered manually and assigned to each other.

For more information about employee handling and administration, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

- Account definitions for user accounts on page 22
- Assigning employees automatically to user accounts on page 43
- Setting deferred deletion for custom target system user accounts on page 54
- Creating and editing user accounts on page 106

Account definitions for user accounts

One Identity Manager has account definitions for automatically allocating user accounts to employees. You can create account definitions for every target system. If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

The data for the user accounts in the respective target system comes from the basic employee data. The employees must have a central user account. The assignment of the IT operating data to the employee's user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role. Processing is done through templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

Specify the manage level for an account definition for managing user accounts. The user account's manage level specifies the extent of the employee's properties that are inherited by the user account. This allows an employee to have several user accounts in one target system, for example:

- Default user account that inherits all properties from the employee.
- Administrative user account that is associated to an employee but should not inherit the properties from the employee.

For more detailed information about the principles of account definitions, manage levels, and determining the valid IT operating data, see the *One Identity Manager Target System Base Module Administration Guide*.

The following steps are required to implement an account definition:

- Creating account definitions
- Configuring manage levels
- Creating the formatting rules for IT operating data
- Collecting IT operating data
- Assigning account definitions to employees and target systems

Detailed information about this topic

- Creating account definitions on page 23
- Editing account definitions on page 23
- Main data for account definitions on page 24
- Editing manage levels on page 26
- Creating manage levels on page 27
- Main data for manage levels on page 29
- Creating mapping rules for IT operating data on page 30
- Entering IT operating data on page 31
- Modify IT operating data on page 32
- Assigning account definitions to employees on page 33
- Assigning account definitions to custom target systems on page 40
- Deleting account definitions on page 40

Creating account definitions

To create a new account definition

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Click in the result list.
3. On the main data form, enter the main data of the account definition.
4. Save the changes.

Detailed information about this topic

- Main data for account definitions on page 24
- Editing account definitions on page 23
- Assigning manage levels to account definitions on page 28

Editing account definitions

To edit an account definition

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.

3. Select the **Change main data** task.
4. Enter the account definition's main data.
5. Save the changes.

Related topics

- Main data for account definitions on page 24
- Creating account definitions on page 23
- Assigning manage levels to account definitions on page 28

Main data for account definitions

Enter the following data for an account definition:

Table 6: Main data for an account definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema that maps user accounts.
Target system	Target system to which the account definition applies.
Required account definition	Specifies the required account definition. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is assigned automatically.
Description	Text field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of assigning the account definition to employees. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Service item	Service item through which you can request the account definition resource in the IT Shop. Assign an existing service item or add a new one.
IT Shop	Specifies whether the account definition can be requested through the IT Shop. The account definition can be requested

Property	Description
	by an employee through the Web Portal and distributed using a defined approval process. The resource can also be assigned directly to employees and roles outside the IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be requested by an employee through the Web Portal and distributed using a defined approval process. The account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is automatically assigned to all internal employees. To automatically assign the account definition to all internal employee, use the **Enable automatic assignment to employees** The account definition is assigned to every employee that is not marked as external. Once a new internal employee is created, they automatically obtain this account definition. To automatically remove the account definition assignment from all employees, use the **Disable automatic assignment to employees**. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently deactivated employees. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily deactivated employees. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.

Property	Description
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk. Option set: The account definition assignment remains in effect. The user account remains intact. Option not set (default): The account definition assignment is not in effect. The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.
System entitlements 1 can be inherited System entitlements 2 can be inherited System entitlements 3 can be inherited	Specifies whether the user account may inherit system entitlements of the corresponding type through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. • For example, if you add an employee with a user account to a department and you have assigned system entitlements to that department, the user account inherits those system entitlements. • If an employee has requested an assignment to a system entitlement in the IT Shop and this request is approved and assigned, then the employee's user account inherits this system entitlement only if the option is enabled.

Editing manage levels

One Identity Manager supplies a default configuration for manage levels:

- **Unmanaged**: User accounts with the **Unmanaged** manage level are linked to the employee but they do no inherit any further properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.
- **Full managed**: User accounts with the **Full managed** manage level inherit defined properties of the assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee's properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

NOTE: The **Full managed** and **Unmanaged** manage levels are analyzed in templates. You can customize the supplied templates in the Designer.

You can define other manage levels depending on your requirements. You need to amend the templates to include manage level approaches.

Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level. For more information about manage levels, see the *One Identity Manager Target System Base Module Administration Guide*.

- Employee user accounts can be locked when they are disabled, deleted, or rated as a security risk so that permissions are immediately withdrawn. If the employee is reinstated at a later date, the user accounts are also reactivated.
- You can also define group membership inheritance. Inheritance can be discontinued if desired when, for example, the employee's user accounts are disabled and therefore cannot be members in groups. During this time, no inheritance processes should be calculated for this employee. Existing group memberships are deleted.

To edit a manage level

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Account definitions > Manage levels** category.
2. Select the manage level in the result list.
3. Select the **Change main data** task.
4. Edit the manage level's main data.
5. Save the changes.

Related topics

- Main data for manage levels on page 29
- Creating manage levels on page 27
- Assigning manage levels to account definitions on page 28

Creating manage levels

One Identity Manager supplies a default configuration for the **Unmanaged** and **Full managed** manage levels. You can define other manage levels depending on your requirements.

IMPORTANT: In the Designer, extend the templates by adding the procedure for the additional manage levels. For more information about templates, see the *One Identity Manager Configuration Guide*

To create a manage level

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Account definitions > Manage levels** category.
2. Click in the result list.
3. On the main data form, edit the main data of the manage level.
4. Save the changes.

Related topics

- Main data for manage levels on page 29
- Editing manage levels on page 26
- Assigning manage levels to account definitions on page 28

Assigning manage levels to account definitions

IMPORTANT: The **Unmanaged** manage level is assigned automatically when you create an account definition and it cannot be removed.

To assign manage levels to an account definition

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign manage level** task.
4. In the **Add assignments** pane, assign the manage level.

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

   To remove an assignment

   - Select the manage level and double-click .
5. Save the changes.

Main data for manage levels

Enter the following data for a manage level.

Table 7: Main data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Text field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • **Never**: Data is not updated. (Default) • **Always**: Data is always updated. • **Only initially**: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily deactivated retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily deactivated employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently deactivated employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently deactivated employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.
Lock user accounts if deletion is deferred	Specifies whether user accounts of employees marked for deletion are locked.
Retain groups on security risk	Specifies whether user accounts of employees posing a security risk retain their group memberships.
Lock user accounts if security is at risk	Specifies whether user accounts of employees posing a security risk are locked.
Retain groups if user account disabled	Specifies whether disabled user accounts retain their group memberships.

Creating mapping rules for IT operating data

An account definition specifies which rules are used to form the IT operating data and which default values will be used if no IT operating data can be found through the employee's primary roles.

The following IT operating data is used in the One Identity Manager default configuration for automatically creating user accounts for an employee in the target system and modifying them.

- Container (per target system)
- Groups can be inherited
- Identity
- Privileged user account.

To create a mapping rule for IT operating data

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Edit IT operating data mapping** task.
4. Click **Add** and enter the following information:
    - **Column**: 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*.
    - **Source**: Specifies which roles to use in order to find the user account properties. You have the following options:
        - Primary department
        - Primary location
        - Primary cost center
        - Primary business roles

          NOTE: The business role can only be used if the Business Roles Module is available.
        - Empty

          If you select a role, you must specify a default value and set the **Always use default value** option.
    - **Default value**: Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.

- **Always use default value**: Specifies whether the user account property is always set with the default value. IT operating data is not determined dynamically from a role.
- **Notify when applying the default**: Specifies whether an email is sent to a specific mailbox when the default value is used. The **Employee - new user account with default properties created** mail template is used.

  To change the mail template, in the Designer, adjust the **TargetSystem | UNS | Accounts | MailTemplateDefaultValues** configuration parameter.

5. Save the changes.

Related topics

- Entering IT operating data on page 31

Entering IT operating data

To create user accounts for an employee 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 employee is assigned a primary business role, primary location, primary department, or primary cost center. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

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

Example:

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

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain A. 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 role in the **Organizations** or **Business roles** category.
2. Select the **Edit IT operating data** task.
3. 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.
    - **Value**: Enter a fixed value to assign to the user account's property.
4. Save the changes.

Related topics

- Creating mapping rules for IT operating data on page 30

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 department, a cost center, a business role, or a location 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 employee to a primary department, cost center, to a primary business role or to a primary location changes, the templates are automatically

run.

To run the template

1. In the Manager, select the **Custom target systems > 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.

Assigning account definitions to employees

Account definitions are assigned to company employees.

Indirect assignment is the default method for assigning account definitions to employees. Account definitions are assigned to departments, cost centers, locations, or roles. The employees are categorized into these departments, cost centers, locations, or roles depending on their function in the company and thus obtain their account definitions. To react quickly to special requests, you can assign individual account definitions directly to employees.

You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. Department managers can then request user accounts from the Web Portal for their staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or added directly to the IT Shop as products.

In the One Identity Manager default installation, the processes are checked at the start to see if the employee already has a user account in the target system that has an account definition. If no user account exists, a new user account is created with the account definition's default manage level.

NOTE: If a user account already exists and is disabled, then it is re-enabled. In this case, you must change the user account manage level afterward.

NOTE: As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted.

Prerequisites for indirect assignment of account definitions to employees

- Assignment of employees and account definitions 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.

For more information about preparing role classes to be assigned, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Detailed information about this topic

- Assigning account definitions to departments, cost centers, and locations on page 34
- Assigning account definitions to business roles on page 35
- Assigning account definitions to all employees on page 36
- Assigning account definitions directly to employees on page 36
- Assigning account definitions to custom target systems on page 40

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition 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.

Related topics

- Assigning account definitions to business roles on page 35
- Assigning account definitions to all employees on page 36
- Assigning account definitions directly to employees on page 36

Assigning account definitions to business roles

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

To add account definitions to hierarchical roles

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition 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.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 34
- Assigning account definitions to all employees on page 36
- Assigning account definitions directly to employees on page 36

Assigning account definitions to all employees

Use this task to assign the account definition to all internal employees. Employees that are marked as external do not obtain this account definition. Once a new internal employee is created, they automatically obtain this account definition. The assignment is calculated by the DBQueue Processor.

IMPORTANT: Only run this task if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.

To assign an account definition to all employees

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Change main data** task.
4. Select the **Disable automatic assignment to employees** task.
5. Confirm the security prompt with **Yes**.
6. Save the changes.

NOTE: To automatically remove the account definition assignment from all employees, run the DISABLE AUTOMATIC ASSIGNMENT TO EMPLOYEES task. The account definition cannot be reassigned to employees from this point on. Existing assignments remain intact.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 34
- Assigning account definitions to business roles on page 35
- Assigning account definitions directly to employees on page 36

Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition 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 account definitions to departments, cost centers, and locations on page 34
- Assigning account definitions to business roles on page 35
- Assigning account definitions to all employees on page 36

Assigning account definitions to system roles

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

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

To add account definitions to a system role

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign system roles** task.
4. 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. Save the changes.

Adding account definitions in the IT Shop

An account definition can be requested by shop customers when it is assigned to an IT Shop shelf. To ensure it can be requested, further prerequisites need to be guaranteed.

- The account definition must be labeled with the **IT Shop** option.
- The account definition must be assigned to a service item.

  TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in the Web Portal, assign a service category to the service item.

- If the account definition is only assigned to employees using IT Shop assignments, you must also set the **Only for use in IT Shop** option. Direct assignment to hierarchical roles may not be possible.

NOTE: IT Shop administrators can assign account definitions to IT Shop shelves if login is role-based. Target system administrators are not authorized to add account definitions in the IT Shop.

To add an account definition to the IT Shop (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

To add an account definition to the IT Shop (non role-based login)

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Add assignments** pane, assign the account definitions to the IT Shop shelves.
5. Save the changes.

To remove an account definition from individual IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.
4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

To remove an account definition from individual IT Shop shelves (non role-based login)

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Add to IT Shop** task.

4. In the **Remove assignments** pane, remove the account definitions from the IT Shop shelves.
5. Save the changes.

To remove an account definition from all IT Shop shelves (role-based login)

1. In the Manager, select the **Entitlements > Account definitions** category.
2. Select an account definition 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 account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

1. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
2. Select an account definition 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 account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

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

Related topics

- Main data for account definitions on page 24
- Assigning account definitions to departments, cost centers, and locations on page 34
- Assigning account definitions to business roles on page 35
- Assigning account definitions directly to employees on page 36
- Assigning account definitions to system roles on page 37

Assigning account definitions to custom target systems

The following prerequisites must be fulfilled if you implement automatic assignment of user accounts and employees resulting in administered user accounts (**Linked configured** state):

- The account definition is assigned to the target system.
- The account definition has the default manage level.

User accounts are only linked to the employee (**Linked** state) if no account definition is given. This is the case on initial synchronization, for example.

To assign the account definition to a target system

1. In the Manager, select the target system in the **Custom target systems** category.
2. Select the **Change main data** task.
3. From the **Account definition (initial)** menu, select the account definition for user accounts.
4. Save the changes.

Automatic assignment of employees to user accounts must be customized for custom target systems.

Detailed information about this topic

- Assigning employees automatically to user accounts on page 43

Deleting account definitions

You can delete account definitions if they are not assigned to target systems, employees, hierarchical roles or any other account definitions.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
    a. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.
    b. Select an account definition in the result list.
    c. Select the **Change main data** task.
    d. Select the **Disable automatic assignment to employees** task.

e. Confirm the security prompt with **Yes**.

f. Save the changes.

2. Remove direct assignments of the account definition to employees.

   a. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.

   b. Select an account definition in the result list.

   c. Select the **Assign to employees** task.

   d. In the **Remove assignments** pane, remove employees.

   e. Save the changes.

3. Remove the account definition's assignments to departments, cost centers, and locations.

   a. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.

   b. Select an account definition in the result list.

   c. Select the **Assign organizations** task.

   d. In the **Remove assignments** pane, remove the relevant departments, cost centers, and locations.

   e. Save the changes.

4. Remove the account definition's assignments to business roles.

   a. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.

   b. Select an account definition in the result list.

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

   d. In the **Remove assignments** pane, remove the business roles.

   e. Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves.

   For more detailed information about unsubscribing requests, see the *One Identity Manager Web Designer Web Portal User Guide*.

   To remove an account definition from all IT Shop shelves (role-based login)

   a. In the Manager, select the **Entitlements > Account definitions** category.

   b. Select an account definition in the result list.

   c. Select the **Remove from all shelves (IT Shop)** task.

   d. Confirm the security prompt with **Yes**.

   e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

To remove an account definition from all IT Shop shelves (non role-based login)

a. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Select the **Remove from all shelves (IT Shop)** task.

d. Confirm the security prompt with **Yes**.

e. Click **OK**.

The account definition is removed from all shelves by the One Identity Manager Service. At the same time, any requests and assignment requests with this account definition are canceled.

6. Remove the required account definition assignment. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.

a. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

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

d. From the **Required account definition** menu, remove the account definition.

e. Save the changes.

7. Remove the account definition's assignments to target systems.

a. In the Manager, select the target system in the **Custom target systems** category.

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

c. On the **General** tab, remove the assigned account definitions.

d. Save the changes.

8. Delete the account definition.

a. In the Manager, select the **Custom target systems > Basic configuration data > Account definitions > Account definitions** category.

b. Select an account definition in the result list.

c. Click to delete an account definition.

Assigning employees automatically to user accounts

When you add a user account, an existing employee can automatically be assigned to it. If necessary, a new employee can be created. The identity's main data is created on the basis of existing user account main data. This mechanism can be triggered after a new user account is created either manually or through synchronization.

Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

If you run this procedure during working hours, automatic assignment of employees to user accounts takes place from that moment onwards. If you disable the procedure again later, the changes only affect user accounts added or updated after this point in time. Existing employee assignments to user accounts remain intact.

NOTE: It is not recommended to assign employees using automatic employee assignment in the case of administrative user accounts. Use **Change main data** to assign employees to administrative user accounts for the respective user account.

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

Run the following tasks to assign employees automatically:

- If you want employees to be assigned during synchronization of user accounts, in the Designer, set the **TargetSystem | UNS | PersonAutoFullsync** configuration parameter and select the required mode.
- If you want employees to be assigned outside synchronization, in the Designer, set the **TargetSystem | UNS | PersonAutoDefault** configuration parameter and select the required mode.
- In the **TargetSystem | UNS | PersonExcludeList** configuration parameter, define the user accounts for which no automatic assignment to employees shall take place.

  Example:

  ```
  ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $
  ```

  TIP: You can edit the value of the configuration parameter in the **Exclude list for automatic employee assignment** dialog.

  To edit the exclude list for automatic employee assignment

  1. In the Designer, edit the **PersonExcludeList** configuration parameter.
  2. Click **...** next to the **Value** field.

     This opens the **Exclude list for user accounts** dialog.

3. To add a new entry, click **Add**.

   To edit an entry, select it and click **Edit**.

4. Enter the name of the user account that does not allow employees to be assigned automatically.

   Each entry in the list is handled as part of a regular expression. You are allowed to use the usual special characters for regular expressions.

5. To delete an entry, select it and click **Delete**.
6. Click **OK**.

- Use the **TargetSystem | UNS | PersonAutoDisabledAccounts** configuration parameter to specify whether employees can be automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
- Assign an account definition to the target system. Ensure that the manage level to be used is entered as the default manage level.
- Define the search criteria for employees assigned to the target system.

  NOTE: To determine the origin of the employees, in the `TSB_PersonAuto_Mapping_UNSAccountB` script, you can fill the `Person.ImportSource` column. To do this, add to the list of permitted values in the Designer in the `Person.ImportSource` column and overwrite the script accordingly.

NOTE:

The following applies for synchronization:

- Automatic employee assignment takes effect if user accounts are added or updated.

The following applies outside synchronization:

- Automatic employee assignment takes effect if user accounts are added.

NOTE:

In the default installation, after synchronizing, employees are automatically created for the user accounts.If an account definition for the target system is not known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

To manage the user accounts using account definitions, assign an account definition and a manage level to these user accounts.

Related topics

- Creating account definitions on page 23
- Assigning account definitions to custom target systems on page 40
- Changing manage levels for user accounts on page 47
- Assigning account definitions to linked user accounts on page 48
- Editing search criteria for automatic employee assignment on page 45

Editing search criteria for automatic employee assignment

The criteria for employee assignments are defined for the target system. You specify which user account properties must match the employee's properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions.

The search criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (`AccountToPersonMatchingRule`) in the target system table.

Search criteria are evaluated when employees are automatically assigned to user accounts. Furthermore, you can create a suggestion list for assignments of employees to user accounts based on the search criteria and make the assignment directly.

NOTE: Object definitions for user accounts that can have search criteria applied to them are predefined. For example, if you require other objects definitions that limit a preselection of user accounts, set up the respective custom object definitions in the Designer. For more information, see the *One Identity Manager Configuration Guide*.

To specify criteria for employee assignment

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Target systems** category.
2. Select the target system in the result list.
3. Select the **Define search criteria for employee assignment** task.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

   Table 8: Search criteria for user accounts

Apply to	Employee column	User account column
User accounts	Central user account (CentralAccount)	Login name (AccountName)

5. Save the changes.

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

Related topics

- Assigning employees automatically to user accounts on page 43
- Finding employees and directly assigning them to user accounts on page 46

Finding employees and directly assigning them to user accounts

Based on the search criteria, you can create a suggestion list for the assignment of employees to user accounts and make the assignment directly. User accounts are grouped in different views for this.

Table 9: Manual assignment view

View	Description
Suggested assignments	This view lists all user accounts to which One Identity Manager can assign an employee. All employees are shown who were found using the search criteria and can be assigned.
Assigned user accounts	This view lists all user accounts to which an employee is assigned.
Without employee assignment	This view lists all user accounts to which no employee is assigned and for which no employee was found using the search criteria.

To apply search criteria to user accounts

TIP: By double-clicking on an entry in the view, you can view the user account and employee main data.

The assignment of employees to user accounts creates connected user accounts (**Linked** state). To create managed user accounts (**Linked configured** state), you can assign an account definition at the same time.

To assign employees directly over a suggestion list

- Click **Suggested assignments**.
    1. Click the **Selection** box of all user accounts to which you want to assign the suggested employees. Multi-select is possible.
    2. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.
    3. Click **Assign selected**.
    4. Confirm the security prompt with **Yes**.

       The employees determined using the search criteria are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

    - OR -
- Click **No employee assignment**.

1. Click **Select employee** for the user account to which you want to assign an employee. Select an employee from the menu.
2. Click the **Selection** box of all user accounts to which you want to assign the selected employees. Multi-select is possible.
3. (Optional) Select an account definition in the **Assign this account definition** menu, and select a manage level in the **Assign this account manage level** menu.
4. Click **Assign selected**.
5. Confirm the security prompt with **Yes**.

   The employees displayed in the **Employee** column are assigned to the selected user accounts. If an account definition was selected, this is assigned to all selected user accounts.

To remove assignments

- Click **Assigned user accounts**.
  1. Click the **Selection** box of all the user accounts you want to delete the employee assignment from. Multi-select is possible.
  2. Click **Remove selected**.
  3. Confirm the security prompt with **Yes**.

     The assigned employees are removed from the selected user accounts.

Changing manage levels for user accounts

The default manage level is applied if you create user accounts using automatic employee assignment. You can change a user account manage level later.

To change the manage level for a user account

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the manage level in the **Manage level** list on the **General** tab.
5. Save the changes.

Assigning account definitions to linked user accounts

An account definition can be subsequently assigned to user accounts with **Linked** status. This may be necessary, for example, if:

- Employees and user accounts were linked manually.
- Automatic employee assignment is configured, but when a user account is inserted, no account definition is assigned in the domain.

To manage user accounts through account definitions

1. Create an account definition.
2. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
    a. In the Manager, select the **Custom Target Systems > target system > User accounts > Linked but not configured > <target system>** category.
    b. Select the **Assign account definition to linked accounts** task.
    c. In the **Account definition** menu, select the account definition.
    d. Select the user accounts that contain the account definition.
    e. Save the changes.

Detailed information about this topic

- Assigning account definitions to custom target systems on page 40

Supported user account types

Different types of user accounts, such as default user accounts, administrative user accounts, service accounts, or privileged user accounts, can be mapped in One Identity Manager.

The following properties are used for mapping different user account types.

- Identity

  The **Identity** property (`IdentityType` column) is used to describe the type of user account.

Table 10: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.	Organizational
Personalized admin identity	User account with administrative permissions, used by one employee.	Admin
Sponsored identity	User account used for a specific purpose. For example, for training purposes.	Sponsored
Shared identity	User account with administrative permissions, used by several employees.	Shared
Service identity	Service account.	Service

NOTE: To enable working with identities for user accounts, the employees also need identities. You can only link user accounts to which an identity is assigned with employees who have this same identity.

The primary identity, the organizational identity, and the personalized admin identity are used for different user accounts, which can be used by the same actual employee to perform their different tasks within the company.

To provide user accounts with a personalized admin identity or an organizational identity for an employee, you create subidentities for the employee. These subidentities are then linked to user accounts, enabling you to assign the required permissions to the different user accounts.

User accounts with a sponsored identity, shared identity, or service identity are linked to pseudo employees that do not refer to a real employee. These pseudo employees are needed so that permissions can be inherited by the user accounts. When evaluating reports, attestations, or compliance checks, check whether pseudo employees need to be considered separately.

For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

- Privileged user account

  Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are labeled with the **Privileged user account** property (`IsPrivilegedAccount` column).

Detailed information about this topic

- Default user accounts on page 50
- Administrative user accounts on page 51
- Providing administrative user accounts for one employee on page 51
- Providing administrative user accounts for several employees on page 52
- Privileged user accounts on page 53

Default user accounts

Normally, each employee obtains a default user account, which has the permissions they require for their regular work. The user accounts are linked to the employee. The effect of the link and the scope of the employee's inherited properties on the user accounts can be configured through an account definition and its manage levels.

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.
2. Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
3. Create a formatting rule for IT operating data.

   You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

   The type of IT operating data required depends on the target system. The following setting are recommended for default user accounts:

   - In the mapping rule for the `IsGroupAccount` column, use the default value **1** and enable the **Always use default value** option.
   - In the mapping rule for the `IdentityType` column, use the default value **Primary** and enable **Always use default value**.
4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

   Specify in the departments, cost centers, locations, or business roles that IT operating data should apply when you set up a user account.
5. Assign the account definition to employees.

   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

Related topics

- Account definitions for user accounts on page 22

Administrative user accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are usually predefined by the target system and have fixed names and login names, such as **Administrator**.

Administrative user accounts are imported into One Identity Manager during synchronization.

NOTE: Some administrative user accounts can be automatically identified as privileged user accounts. To do this, in the Designer, enable the **Mark selected user accounts as privileged** schedule.

Related topics

- Providing administrative user accounts for one employee on page 51
- Providing administrative user accounts for several employees on page 52

Providing administrative user accounts for one employee

Prerequisites

- The user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be labeled as a personalized admin identity.
- The employee who will be using the user account must be linked to a main identity.

To prepare an administrative user account for a person

1. Label the user account as a personalized admin identity.
    a. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
    b. Select the user account in the result list.
    c. Select the **Change main data** task.
    d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.
2. Link the user account to the employee who will be using this administrative user account.

a. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.

b. Select the user account in the result list.

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

d. On the **General** tab, in the **Person** selection list, select the employee who will be using this administrative user account.

TIP: If you are the target system manager, you can choose to create a new person.

Related topics

- Providing administrative user accounts for several employees on page 52
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several employees

Prerequisite

- The user account must be labeled as a shared identity.
- A pseudo employee must exist. The pseudo employee must be labeled as a shared identity and must have a manager.
- The employees who are permitted to use the user account must be labeled as a primary identity.

To prepare an administrative user account for multiple employees

1. Label the user account as a shared identity.
   a. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
   b. Select the user account in the result list.
   c. Select the **Change main data** task.
   d. On the **General** tab, in the **Identity** menu, select **Shared identity**.
2. Link the user account to a pseudo employee.
   a. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
   b. Select the user account in the result list.
   c. Select the **Change main data** task.
   d. On the **General** tab, select the pseudo employee from the **Employee** menu.

TIP: If you are the target system manager, you can choose to create a new pseudo employee.

3. Assign the employees who will use this administrative user account to the user account.
   a. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
   b. Select the user account in the result list.
   c. Select the **Assign employees authorized to use** task.
   d. 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 .

Related topics

- Providing administrative user accounts for one employee on page 51
- For more information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are labeled with the **Privileged user account** property (`IsPrivilegedAccount` column).

NOTE: The criteria according to which user accounts are automatically identified as privileged are defined as extensions to the view definition (ViewAddOn) in the `TSBVAccountIsPrivDetectRule` table (which is a table of the **Union** type). The evaluation is done in the `TSB_SetIsPrivilegedAccount` script.

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.
2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts are created.
3. Specify the effect of temporarily or permanently disabling or deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
4. Create a formatting rule for the IT operating data.

You use the mapping rule to define which rules are used to map IT operating data for user accounts and which default values are used if no IT operating data can be determined through a person's primary roles.

The type of IT operating data required depends on the target system. The following settings are recommended for privileged user accounts:

- In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and set the **Always use default value** option.
- You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.
- To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and set the **Always use default value** option.

5. Enter the effective IT operating data for the target system.

   Specify in the departments, cost centers, locations, or business roles which IT operating data should apply when you set up a user account.

6. Assign the account definition directly to employees who work with privileged user accounts.

   When the account definition is assigned to an employee, a new user account is created through the inheritance mechanism and subsequent processing.

TIP: If customization requires that the login names of privileged user accounts follow a defined naming convention, specify how the login names are formatted in the template.

Related topics

- Account definitions for user accounts on page 22

Setting deferred deletion for custom target system user accounts

You can use deferred deletion to specify how long the user accounts remain in the database after deletion is triggered before they are finally removed. By default, user accounts are finally deleted from the database after 30 days. First, the user accounts are disabled or blocked. You can reenable the user accounts up until deferred deletion runs. After deferred deletion is run, the user accounts are deleted from the database and cannot be restored anymore.

You have the following options for configuring deferred deletion.

- Global deferred deletion: Deferred deletion applies to user accounts in all target system. The default value is **30** days.

  In the Designer, enter a different value for deferred deletion in the **Deferred deletion [days]** property of the `UNSAccountB` table.

- Target system specific deferred deletion: Deferred deletion can be configured individually for each target system. This deferred deletion overrides global deferred deletion.

  To enable deferred deletion separately for each target system

  1. In the Manager, configure deferred deletion for the target system.
     a. In the Manager, select the **Custom Target Systems > Basic configuration data > Target systems** category.
     b. In the result list, select a target system and run the **Change main data** task.
     c. On the **General** tab, under **Deferred deletion [days]**, enter the deferred deletion value in days.
     d. Save the changes.
  2. In the Designer, create a **Script (deferred deletion)** in the `UNSAccountB` table.

     Example:

     Deferred deletion of user accounts in a custom target system depends on the deferred deletion of the target system (`UNSRootB.DeleteDelayDays`). The following script is given in the `UNSAccountB` table.

     ```
     If $FK(UID_UNSRootB).DeleteDelayDays:Int$ > 0 Then
          Value = $FK(UID_UNSRootB).DeleteDelayDays:Int$
     End If
     ```

- Object-specific deferred deletion: Deferred deletion can be configured depending on certain properties of the accounts.

  To use object-specific deferred deletion, in the Designer, create a **Script (deferred deletion)** for the `UNSAccountB` table.

  Example:

  Deferred deletion of privileged user accounts is 10 days. The following **Script (deferred deletion)** is entered in the table.

  ```
  If Not $IsPrivilegedAccount:Bool$ Then
       Value = 10
  End If
  ```

For more information on editing table definitions and configuring deferred deletion in the Designer, see the *One Identity Manager Configuration Guide*.

Related topics

- General main data for custom target systems on page 100
- Deleting and restoring user accounts on page 114

Managing assignments of groups and system entitlements

Groups and system entitlements represent the objects used in the target system to control access to target system resources. A user account obtains the required permissions for accessing target system resources through its memberships in groups and system entitlements.

In One Identity Manager, you can assign groups and system entitlements directly to user accounts or they can be inherited through departments, cost centers, locations, or business roles. Users can also request the groups and system entitlements through the Web Portal. To do this, groups and system entitlements are provided in the IT Shop.

Detailed information about this topic

- Specifying types of system entitlements in use on page 57
- Assigning groups and system entitlements to user accounts in One Identity Manager on page 60
- Effectiveness of memberships in groups and system entitlements on page 78
- Inheriting groups and system entitlements based on categories on page 81
- Overview of all assignments on page 83

Specifying types of system entitlements in use

Many target systems use more than one group type to map entitlements. For example, these might be groups, roles, or entitlement sets. There are four different types mapped in One Identity Manager

Table 11: Types of system entitlements used

Type	Table
Groups	UNSGroupB
System entitlements 1	UNSGroupB1
System entitlements 2	UNSGroupB2
System entitlements 3	UNSGroupB3

You decide when you set up synchronization, which types are mapped in which tables.

A user account obtains the required entitlements for accessing target system resources through its assignments to groups or system entitlements. Depending on the target system, assignments are maintained either on user accounts (user-based assignment) or on groups or system entitlements (entitlement-based assignment). In One Identity Manager, you can configure the behavior accordingly. Memberships are stored in the following tables:

Table 12: User-based assignment

UNSAccountBHasUNSGroupB	**Groups: Assignments to user accounts**
UNSAccountBHasUNSGroupB1	**System entitlements 1: Assignments to user accounts**
UNSAccountBHasUNSGroupB2	**System entitlements 2: Assignments to user accounts**
UNSAccountBHasUNSGroupB3	**System entitlements 3: Assignments to user accounts**

Table 13: Entitlement-based assignment

UNSAccountBInUNSGroupB	**User accounts: Assignment to groups**
UNSAccountBInUNSGroupB1	**User accounts: Assignment to system entitlements 1**
UNSAccountBInUNSGroupB2	**User accounts: Assignment to system entitlements 2**
UNSAccountBInUNSGroupB3	**User accounts: Assignment to system entitlements 3**

To specify which types of system entitlements to use

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Target systems** category.
2. In the result list, select a target system and run the **Change main data** task.
3. In the **System entitlement types used** menu, select all the types to use in the connected target system.

4. In the **User account contains memberships** menu, select all the types with saved user account assignments.
    a. Enable the system entitlements with saved user account assignments.
    b. Disable the system entitlements with saved system entitlements assignments.
5. Save the changes.

Example

In a target system, entitlements are managed as groups and profiles. Assignments to groups are maintained on the group objects, assignments to profiles on the user accounts. In the One Identity Manager, groups are mapped in the `UNSGroupsB` table, profiles in the `UNSGroupB1` table.

- In the **Types of system entitlements used** menu, set the **Group** and **System entitlement 1** values.
- In the **User account contains memberships** menu, only set the **System entitlement 1** value.

This saves the assignments to system entitlement in the `UNSAccountBHasUNSGroupB1`, and `UNSAccountBInUNSGroupB` tables.

NOTE: When setting up attestation procedures, compliance rules, or company policies using system entitlements, be sure to select the correct assignment tables to look at both user-based and entitlement-based assignments.

To set up functions independently of the target system configurations, use the target system mapping in the Unified Namespace. Both user-based and entitlement-based assignments for all types of system entitlements are mapped in the `UNSAccountInUNSGroup` table; the `UNSGroup` table contains all system entitlements regardless of type.

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

Detailed information about the attestation functions, compliance rules, and company policies can be found in the following guides:

One Identity Manager Attestation Administration Guide
One Identity Manager Compliance Rules Administration Guide
One Identity Manager Company Policies Administration Guide

Related topics

- General main data for custom target systems on page 100

Assigning groups and system entitlements to user accounts in One Identity Manager

Groups and system entitlements can be assigned directly or indirectly to a user account. Indirect assignment is carried out by sorting the employee, and the groups and system entitlements into hierarchical roles, such as departments, cost centers, locations, or business roles. If the employee has a user account in the target system, the groups and system entitlements in the role are inherited by this user account. You can assign groups and system entitlements to user accounts that belong to the same target system or to different target systems with the same target system type. For more information, see Target system types for custom target systems on page 136.

Groups and system entitlements can also be requested in the Web Portal. To do this, add employees to a shop as customers. All groups and system entitlements assigned to this shop as products can be requested by the customers. After approval is granted, requested groups and system entitlements are assigned to the employees.

Through system roles, groups and system entitlements can be grouped together and assigned to employees and workdesks as a package. You can create system roles that contain only groups or system entitlements. You can also group any number of company resources into a system role.

To react quickly to special requests, you can assign groups and system entitlements directly to user accounts.

Topic	Guide
Basic principles for assigning and inheriting company resources	*One Identity Manager Identity Management Base Module Administration Guide* *One Identity Manager Business Roles Administration Guide*
Assigning company resources through IT Shop requests	*One Identity Manager IT Shop Administration Guide*
System roles	*One Identity Manager System Roles Administration Guide*

Detailed information about this topic

- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Assigning groups to departments, cost centers, and locations on page 62
- Assigning groups to business roles on page 65
- Adding groups to system roles on page 68

- Adding groups to the IT Shop on page 70
- Assigning user accounts directly to a group on page 74
- Assigning groups directly to user accounts on page 76
- Assigning system entitlements to departments, cost centers, and locations on page 64
- Assigning system entitlements to business roles on page 66
- Adding system entitlements to system roles on page 68
- Adding system entitlements to the IT Shop on page 71
- Assigning user accounts directly to a system entitlement on page 75
- Assigning system entitlements directly to a user account on page 77

Prerequisites for indirect assignments of groups and system entitlements to user accounts

Indirect assignment places employees, groups, and system entitlements into hierarchical roles, such as departments, cost centers, locations, or business roles. When assigning groups and system entitlements indirectly, check the following settings and modify them if necessary.

1. Employee, group, and system entitlement assignment is permitted for role classes (department, cost center, location, or business roles).

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

   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.
2. Settings for assigning groups and system entitlements to user accounts.

- The user account is linked to an employee.
- The options **Groups can be inherited**, **System entitlements 1 can be inherited**, **System entitlements 1 can be inherited**, **System entitlements 1 can be inherited** are set on the user account.
- Depending on the target system type configuration, groups and system entitlements can only be assigned to either user accounts that belong to the same target system or to user accounts that belong to different target systems. For more information, see Target system types for custom target systems on page 136.

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

- Creating and editing user accounts on page 106
- User account main data on page 107
- Groups in custom target systems on page 115
- Main data for groups on page 116
- System entitlements in custom target systems on page 119
- System entitlement main data on page 120

Assigning groups to departments, cost centers, and locations

Assign a group to departments, cost centers, or locations so that the group can be inherited by user accounts through these organizations.

To assign a group to departments, cost centers, or locations (non role-based login)

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group 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.

To assign groups to a department, a cost center, or a location (non role-based login or role-based login)

1. In the Manager, select the **Organizations > Departments** category.

   - OR -

   In the Manager, select the **Organizations > Cost centers** category.

   - OR -

   In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign custom target system entitlements** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .
6. Save the changes.

Related topics

- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Assigning system entitlements to departments, cost centers, and locations on page 64
- Assigning groups to business roles on page 65
- Adding groups to system roles on page 68
- Adding groups to the IT Shop on page 70
- Assigning user accounts directly to a group on page 74
- Assigning groups directly to user accounts on page 76

Assigning system entitlements to departments, cost centers, and locations

Assign a system entitlement to departments, cost centers, or location such that the system entitlement can be inherited by user accounts through these organizations.

To assign a system entitlement to a department, cost center, or location (non role-based login)

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.
2. Select the system entitlement 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.

To assign system entitlements to a department, a cost center, or a location (non role-based login or role-based login)

1. In the Manager, select the **Organizations > Departments** category.

   - OR -

   In the Manager, select the **Organizations > Cost centers** category.

   - OR -

   In the Manager, select the **Organizations > Locations** category.
2. Select the department, cost center, or location in the result list.
3. Select the **Assign custom target system entitlements** task.
4. In the **Add assignments** pane, assign the system entitlements.

- On the **System entitlement 1** tab, assign the system entitlement 1.
- On the **System entitlement 2** tab, assign the system entitlement 2.
- On the **System entitlement 3** tab, assign the system entitlement 3.

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

To remove an assignment

- Select the system entitlement and double-click ✓.

5. Save the changes.

Related topics

- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Assigning groups to departments, cost centers, and locations on page 62
- Assigning system entitlements to business roles on page 66
- Adding system entitlements to system roles on page 68
- Adding system entitlements to the IT Shop on page 71
- Assigning user accounts directly to a system entitlement on page 75
- Assigning system entitlements directly to a user account on page 77

Assigning groups to business roles

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

Assign the group to business roles so that the group is inherited by user accounts through these business roles.

To assign a group to a business role (non role-based login)

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group 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.

To assign groups to a business role (non role-based login or role-based login)

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign groups of custom target systems** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign the groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Related topics

- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Assigning system entitlements to business roles on page 66
- Assigning groups to departments, cost centers, and locations on page 62
- Adding groups to system roles on page 68
- Adding groups to the IT Shop on page 70
- Assigning user accounts directly to a group on page 74
- Assigning groups directly to user accounts on page 76

Assigning system entitlements to business roles

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

Assign a system entitlement to business roles such that the group is inherited by user accounts through these business roles.

To assign a system entitlement to business roles (non role-based login):

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.

2. Select the system entitlement 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.

To assign system entitlements to a business role (non role-based login or role-based login)

1. In the Manager, select the **Business roles > <role class>** category.
2. Select the business role in the result list.
3. Select the **Assign custom target system entitlements** task.
4. In the **Add assignments** pane, assign the system entitlements.
   - On the **System entitlement 1** tab, assign the system entitlement 1.
   - On the **System entitlement 2** tab, assign the system entitlement 2.
   - On the **System entitlement 3** tab, assign the system entitlement 3.

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

   To remove an assignment

   - Select the system entitlement and double-click ✓.
5. Save the changes.

Related topics

- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Assigning groups to business roles on page 65
- Assigning system entitlements to departments, cost centers, and locations on page 64
- Adding system entitlements to system roles on page 68
- Adding system entitlements to the IT Shop on page 71
- Assigning user accounts directly to a system entitlement on page 75
- Assigning system entitlements directly to a user account on page 77

Adding groups to system roles

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

Use this task to add a group to system roles.

If you assign a system role to employees, all custom target system user accounts owned by these employees inherit the group.

NOTE: Groups with **Only use in IT Shop** set can only be assigned to system roles that also have this option set. For more information, see the *One Identity Manager System Roles Administration Guide*.

To assign a group to system roles

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign system roles** task.
4. 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. Save the changes.

Related topics

- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Adding system entitlements to system roles on page 68
- Assigning groups to departments, cost centers, and locations on page 62
- Assigning groups to business roles on page 65
- Adding groups to the IT Shop on page 70
- Assigning user accounts directly to a group on page 74
- Assigning groups directly to user accounts on page 76

Adding system entitlements to system roles

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

Use this task to add a system entitlement to system roles.

If you assign a system role to employees, all custom target system user accounts owned by these employees inherit the system entitlement.

NOTE: System entitlements with **Only use in IT Shop** set can only be assigned to system roles that also have this option set. For more information, see the *One Identity Manager System Roles Administration Guide*.

To assign a system entitlement to system roles

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **Assign system roles** task.
4. 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. Save the changes.

Related topics

- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Adding groups to system roles on page 68
- Assigning system entitlements to departments, cost centers, and locations on page 64
- Assigning system entitlements to business roles on page 66
- Adding system entitlements to the IT Shop on page 71
- Assigning user accounts directly to a system entitlement on page 75
- Assigning system entitlements directly to a user account on page 77

Adding groups to the IT Shop

When you assign a group to an IT Shop shelf, it can be requested by the shop customers. To ensure it can be requested, further prerequisites need to be guaranteed:

- The group must be labeled with the **IT Shop** option.
- The group must be assigned a service item.

  TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the group easier to find in the Web Portal, assign a service category to the service item.
- If you only want the group to be assigned to employees through IT Shop requests, the group must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

NOTE: With role-based login, the IT Shop administrators can assign groups to IT Shop shelves. Target system administrators are not authorized to add groups to IT Shop.

To add a group to the IT Shop.

1. In the Manager, select the **Custom Target Systems > <Target system> > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Custom Target System groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Add assignments** pane, assign the group to the IT Shop shelves.
6. Save the changes.

To remove a group from individual shelves of the IT Shop

1. In the Manager, select the **Custom Target Systems > <Target system> > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Custom Target System groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Remove assignments** pane, remove the group from the IT Shop shelves.
6. Save the changes.

To remove a group from all shelves of the IT Shop

1. In the Manager, select the **Custom Target Systems > <Target system> > Groups** (non role-based login) category.

   - OR -

   In the Manager, select the **Entitlements > Custom Target System groups** (role-based login) category.
2. In the result list, select the group.
3. Select the **Remove from all shelves (IT Shop)** task.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

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

Related topics

- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Main data for groups on page 116
- Adding system entitlements to the IT Shop on page 71
- Assigning groups to departments, cost centers, and locations on page 62
- Assigning groups to business roles on page 65
- Adding groups to system roles on page 68
- Assigning user accounts directly to a group on page 74
- Assigning groups directly to user accounts on page 76

Adding system entitlements to the IT Shop

Once a system entitlement has been assigned to an IT Shop shelf, it can be requested by the shop's customers. To ensure it can be requested, further prerequisites need to be guaranteed.

- The system entitlement must be labeled with the **IT Shop** option.
- The system entitlement must be assigned to a service item.

  TIP: In the Web Portal, all products that can be requested are grouped together by service category. To make the system entitlement easier to find in the Web Portal, assign a service category to the service item.

- If the system entitlement can only be assigned to employees using IT Shop requests, the system entitlement must be also labeled with the **Only use in IT Shop** option. Direct assignment to hierarchical roles or user accounts is then no longer permitted.

NOTE: IT Shop administrators can assign system entitlements to IT Shop shelves if login is role-based. Target system administrators are not authorized to add system entitlements to the IT Shop.

To add a system entitlement to the IT Shop

1. Non role-based login:

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.

   Role-based login:

   In the Manager, select the **Entitlements > Custom Target Systems system entitlements 1** category.

   - OR -

   In the Manager, select the **Entitlements > Custom Target Systems system entitlements 2** category.

   - OR -

   In the Manager, select the **Entitlements > Custom Target Systems system entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Add assignments** pane, assign the system entitlement to IT Shop shelves.
6. Save the changes.

To remove a system entitlement from individual IT Shop shelves

1. Non role-based login:

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

- OR -

In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.

Role-based login:

In the Manager, select the **Entitlements > Custom Target Systems system entitlements 1** category.

- OR -

In the Manager, select the **Entitlements > Custom Target Systems system entitlements 2** category.

- OR -

In the Manager, select the **Entitlements > Custom Target Systems system entitlements 3** category.

2. Select the system entitlement in the result list.
3. Select the **Add to IT Shop** task.
4. Select the **IT Shop structures** tab.
5. In the **Remove assignments** pane, remove the system entitlement from the IT Shop shelves.
6. Save the changes.

To remove a system entitlement from all IT Shop shelves

1. Non role-based login:

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.

   Role-based login:

   In the Manager, select the **Entitlements > Custom Target Systems system entitlements 1** category.

   - OR -

   In the Manager, select the **Entitlements > Custom Target Systems system entitlements 2** category.

   - OR -

In the Manager, select the **Entitlements > Custom Target Systems system entitlements 3** category.

2. Select the system entitlement 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 entitlement is removed from all shelves by the One Identity Manager Service. All requests and assignment requests with this system entitlement are unsubscribed in the process.

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

Related topics

- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Main data for groups on page 116
- Adding groups to the IT Shop on page 70
- Assigning system entitlements to departments, cost centers, and locations on page 64
- Assigning system entitlements to business roles on page 66
- Adding system entitlements to system roles on page 68
- Assigning user accounts directly to a system entitlement on page 75
- Assigning system entitlements directly to a user account on page 77

Assigning user accounts directly to a group

To react quickly to special requests, you can assign groups directly to user accounts. You cannot directly assign groups that have the **Only use in IT Shop** option.

To assign user accounts directly to a group

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

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

To remove an assignment

- Select the user account and double-click ✓.

5. Save the changes.

Related topics

- Assigning user accounts directly to a system entitlement on page 75
- Assigning groups to departments, cost centers, and locations on page 62
- Assigning groups to business roles on page 65
- Adding groups to system roles on page 68
- Adding groups to the IT Shop on page 70
- Assigning groups directly to user accounts on page 76
- Target system types for custom target systems on page 136

Assigning user accounts directly to a system entitlement

To react quickly to special requests, you can assign the system entitlements directly to user accounts. You cannot directly assign system entitlements that have the **Only use in IT Shop** option set.

To assign user accounts directly to a system entitlement

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

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

   To remove an assignment

   - Select the user account and double-click ✓.
5. Save the changes.

Related topics

- Assigning user accounts directly to a group on page 74
- Assigning system entitlements to departments, cost centers, and locations on page 64
- Assigning system entitlements to business roles on page 66
- Adding system entitlements to system roles on page 68
- Adding system entitlements to the IT Shop on page 71
- Assigning system entitlements directly to a user account on page 77
- Target system types for custom target systems on page 136

Assigning groups directly to user accounts

To react quickly to special requests, you can assign groups directly to the user account. You cannot directly assign groups that have the **Only use in IT Shop** option set.

To assign groups directly to user accounts

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign groups and system entitlements** task.
4. Select the **Groups** tab.
5. In the **Add assignments** pane, assign the groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
6. Save the changes.

Related topics

- Assigning system entitlements directly to a user account on page 77
- Assigning groups to departments, cost centers, and locations on page 62
- Assigning groups to business roles on page 65
- Adding groups to system roles on page 68
- Adding groups to the IT Shop on page 70
- Assigning user accounts directly to a group on page 74
- Target system types for custom target systems on page 136

Assigning system entitlements directly to a user account

To react quickly to special requests, you can assign system entitlements directly to a user account. You cannot directly assign system entitlements that have the **Only use in IT Shop** option set.

To assign system entitlements directly to a user account

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign groups and system entitlements** task.
4. Select the **System entitlements 1** tab.

   - OR -

   Select the **System entitlements 2** tab.

   - OR -

   Select the **System entitlements 3** tab.
5. In the **Add assignments** pane, assign the system entitlements.

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

   To remove an assignment

   - Select the system entitlement and double-click .
6. Save the changes.

Related topics

- Assigning groups directly to user accounts on page 76
- Assigning system entitlements to departments, cost centers, and locations on page 64
- Assigning system entitlements to business roles on page 66
- Adding system entitlements to system roles on page 68
- Adding system entitlements to the IT Shop on page 71
- Assigning user accounts directly to a system entitlement on page 75
- Target system types for custom target systems on page 136

Effectiveness of memberships in groups and system entitlements

NOTE: The functionality described here for groups applies equally to system entitlements.

When groups are assigned to user accounts an employee may obtain two or more groups, which are not permitted in this combination. To prevent this, you can declare mutually exclusive groups. To do this, you specify which of the two groups should apply to the user accounts if both are assigned.

It is possible to assign an excluded group at any time either directly, indirectly, or with an IT Shop request. One Identity Manager determines whether the assignment is effective.

NOTE:

- You cannot define a pair of mutually exclusive groups. That means, the definition "Group A excludes group B" `AND` "Group B excludes groups A" is not permitted.
- You must declare each group to be excluded from a group separately. Exclusion definitions cannot be inherited.
- One Identity Manager does not check if membership of an excluded group is permitted in another group (`UNSGroupBInUNSGroupB` table).

The effectiveness of the assignments is mapped in the `UNSAccountBInUNSGroupB`/`UNSAccountBHasUNSGroupB` and `BaseTreeHasUNSGroupB` tables by the `XIsInEffect` column.

Example: The effect of group memberships

- Group A is defined with permissions for triggering requests in a target system. A group B is authorized to make payments. A group C is authorized to check invoices.
- Group A is assigned through the "Marketing" department, group B through "Finance", and group C through the "Control group" business role.

Jo User1 has a user account in this target system. They primarily belong to the "Marketing" department. The "Control group" business role and the "Finance" department are assigned to them secondarily. Without an exclusion definition, the user account obtains all the permissions of groups A, B, and C.

By using suitable controls, you want to prevent an employee from being able to trigger a request and to pay invoices. That means, groups A, B, and C are mutually exclusive. An employee that checks invoices may not be able to make invoice payments as well. That means, groups B and C are mutually exclusive.

Table 14: Specifying excluded groups (`UNSGroupBExclusion` table)

Effective group	Excluded group
Group A	
Group B	Group A
Group C	Group B

Table 15: Effective assignments

Employee	Member in role	Effective group
Pat Identity1	Marketing	Group A
Jan User3	Marketing, finance	Group B
Jo User1	Marketing, finance, control group	Group C
Chris User2	Marketing, control group	Group A, Group C

Only the group C assignment is in effect for Jo User1. It is published in the target system. If Jo User1 leaves the "control group" business role at a later date, group B also takes effect.

The groups A and C are in effect for Chris User2 because the groups are not defined as mutually exclusive. That means that the employee is authorized to trigger requests and to check invoices. If this should not be allowed, define further exclusion for group C.

Table 16: Excluded groups and effective assignments

Employee	Member in role	Assigned group	Excluded group	Effective group
Chris User2	Marketing	Group A		Group C
	Control group	Group C	Group B	
			Group A	

Prerequisites

- The **QER | Structures | Inherite | GroupExclusion** 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*.

- Mutually exclusive groups belong to the same target system or the same target system type.

NOTE: Groups that are mutually exclusive, are determined within a target system type independently of the target system. The features must be taken into account in the definition of exclusion.

To exclude a group

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select a group in the result list.
3. Select the **Exclude groups** task.
4. In the **Add assignments** pane, assign the groups that are mutually exclusive to the selected group.

   - OR -

   In the **Remove assignments** pane, remove the groups that are no longer mutually exclusive.
5. Save the changes.

To exclude system entitlements

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.
2. Select a system entitlement in the result list.
3. Select the **Exclude system entitlements 1** task, **Exclude system entitlements 2** task, or **Exclude system entitlements 3** task to match the selected system entitlement.
4. In the **Add assignments** pane, assign system entitlements that are mutually exclusive to the selected system entitlement.

   - OR -

   In the **Remove assignments** pane, remove the system entitlements that are no longer mutually exclusive.
5. Save the changes.

Inheriting groups and system entitlements based on categories

NOTE: The functionality described here for groups applies equally to system entitlements.

In One Identity Manager, user accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

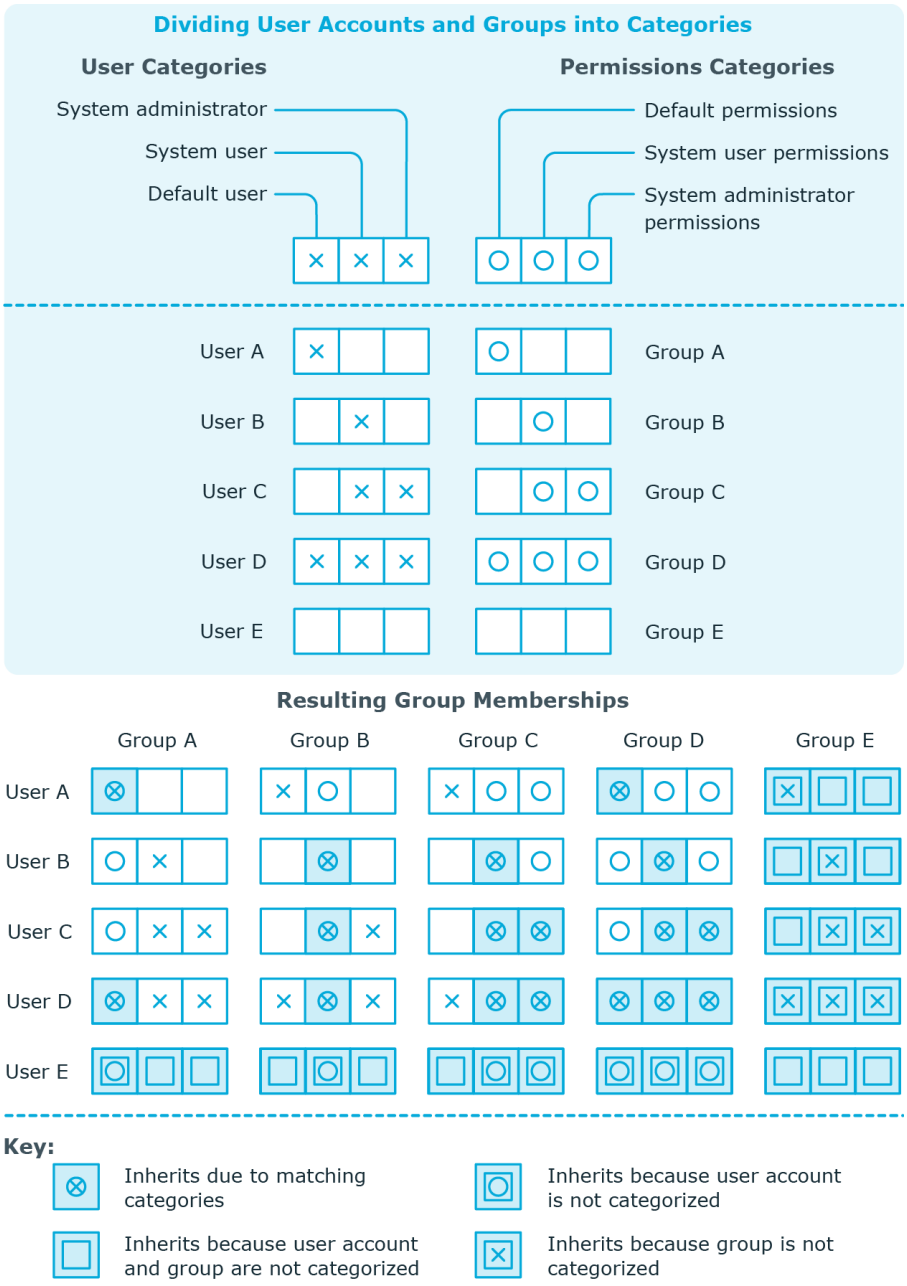
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category items matches an assigned group. The group is also inherited by the user account if the group or the user account is not put into categories.

NOTE: Inheritance through categories is only taken into account when groups are assigned indirectly through hierarchical roles. Categories are not taken into account when groups are directly assigned to user accounts.

Table 17: Category examples

Category item	Categories for user accounts	Categories for groups
1	Default user	Default permissions
2	System users	System user permissions
3	System administrator	System administrator permissions

Figure 1: Example of inheriting through categories.



To use inheritance through categories

- In the Manager, define the categories in the target system.
- Assign categories to user accounts through their main data.
- Assign categories to groups and system entitlements through their main data.

Related topics

- Defining categories for inheriting groups and system entitlements on page 103
- User account main data on page 107
- Main data for groups on page 116
- System entitlement main data on page 120

Overview of all 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 employees who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Examples:

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

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the **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 employees with the selected base object.

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the icon in the report's toolbar.

- Double-click a control to show all child roles belonging to the selected role.
- By clicking the button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to to start a wizard that allows you to bookmark this list of employees for tracking. This creates a new business role to which the employees are assigned.

Figure 2: Toolbar of the Overview of all assignments report.

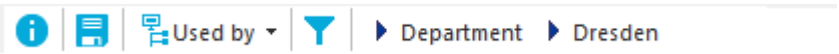


Table 18: Meaning of icons in the report toolbar

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.

Login information for user accounts

When new user accounts are created in One Identity Manager, the passwords needed to log in to the target system are created immediately also. Various options are available for assigning the initial password. Predefined password policies are applied to the passwords, and you can adjust these policies to suit your individual requirements if necessary. You can set up email notifications to distribute the login information generated to users.

Detailed information about this topic

- Password policies for user accounts on page 85
- Initial password for new user accounts on page 97
- Email notifications about login data on page 97

Password policies for user accounts

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

Detailed information about this topic

- Predefined password policies on page 86
- Using password policies on page 87
- Editing password policies on page 88
- Creating password policies on page 89
- Custom scripts for password requirements on page 93
- Editing the password excluded list on page 96
- Verifying passwords on page 96

- Testing password generation on page 96
- Using password policies on page 87

Predefined password policies

You can customize predefined password policies to meet your own requirements if necessary.

Password for logging in to One Identity Manager

The **One Identity Manager password policy** is applied for logging in to One Identity Manager. This password policy defines the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the passcode for a one time log in on the Web Portal (`Person.Passcode`).

NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

For more information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The **Employee central password policy** defines the settings for the (`Person.CentralPassword`) central password. Members of the **Identity Management | Employees | Administrators** application role can adjust this password policy.

IMPORTANT: Ensure that the **Employee central password policy** does not violate the target system-specific requirements for passwords.

For more information about password policies for employees, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Password policies for user accounts

Predefined password policies are provided, which you can apply to the user account password columns of the user accounts.

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

There is no password policy predefined for custom target systems. Create your own password policy and apply it to the custom target system user accounts (`UNSAccountB.UserPassword`).

It is recommended that you set up your own password policy for every custom target system. You can also assign password policies at container level.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

Using password policies

There is no password policy predefined for custom target systems. Create your own password policy and apply it to the custom target system user accounts (`UNSAccountB.UserPassword`).

It is recommended that you set up your own password policy for every custom target system. You can also assign password policies at container level.

Furthermore, you can apply password policies based on the account definition of the user accounts or based on the manage level of the user accounts.

The password policy that is to be used for a user account is determined in the following sequence:

1. Password policy of the user account's account definition.
2. Password policy of the user account's manage level.
3. Password policy of the user account's container.
4. Password policy of the user account's target system.
5. The **One Identity Manager password policy** (default policy).

IMPORTANT: If you do not use password policies that are specific to the target system, the **One Identity Manager password policy** default policy applies. In this case, ensure that the default policy does not violate the target systems requirements.

To reassign a password policy

1. In the Manager, select the **Custom target systems > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.
    - **Apply to**: Application scope of the password policy.

      To specify an application scope

      1. Click → next to the field.
      2. Select one of the following references under **Table**:
          - The table that contains the base objects of synchronization.
          - To apply the password policy based on the account definition, select the **TSBAccountDef** table.

- To apply the password policy based on the manage level, select the **TSBBehavior** table.

3. Under **Apply to**, select the table that contains the base objects.
   - If you have selected the table containing the base objects of synchronization, next select the specific target system.
   - If you have selected the **TSBAccountDef** table, next select the specific account definition.
   - If you have selected the **TSBBehavior** table, next select the specific manage level.
4. Click **OK**.

- **Password column**: Name of the password column.
- **Password policy**: Name of the password policy to use.

5. Save the changes.

To change a password policy's assignment

1. In the Manager, select the **Custom target systems > Basic configuration data > Password policies** category.
2. Select the password policy in the result list.
3. Select the **Assign objects** task.
4. In the **Assignments** pane, select the assignment you want to change.
5. From the **Password Policies** menu, select the new password policy you want to apply.
6. Save the changes.

Editing password policies

Predefined password policies are supplied with the default installation that you can use or customize if required.

To edit a password policy

1. In the Manager, select the **Custom target systems > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Edit the password policy's main data.
5. Save the changes.

Detailed information about this topic

- General main data of password policies on page 89
- Policy settings on page 90
- Character classes for passwords on page 91
- Custom scripts for password requirements on page 93

Creating password policies

Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

To create a password policy

1. In the Manager, select the **Custom target systems > Basic configuration data > Password policies** category.
2. Click in the result list.
3. On the main data form, enter the main data of the password policy.
4. Save the changes.

Detailed information about this topic

- General main data of password policies on page 89
- Policy settings on page 90
- Character classes for passwords on page 91
- Custom scripts for password requirements on page 93

General main data of password policies

Enter the following main data of a password policy.

Table 19: main data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the button.
Description	Text field for additional explanation. Translate the given text using the button.
Error Message	Custom error message generated if the policy is not fulfilled.

Property	Meaning
	Translate the given text using the button.
Owner (Application Role)	Application roles whose members can configure the password policies.
Default policy	Mark as default policy for passwords. This option cannot be changed. NOTE: The **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

Policy settings

Define the following settings for a password policy on the **Password** tab.

Table 20: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have. If the value is **0**, no password is required.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.
Max. errors	Maximum number of errors. Set the number of invalid passwords attempts. The number of failed logins is only taken into account when logging in to One Identity Manager. If the value is **0**, the number of failed logins is not taken into account. This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has exceeded the maximum number of failed logins, the employee or system user will not be able to log in to One Identity Manager. You can use the Password Reset Portal to reset the passwords

Property	Meaning
	of employees and system users who have been blocked. For more information, see the *One Identity Manager Web Designer Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires. If the value is **0**, then the password does not expire.
Password history	Enter the number of passwords to be saved. If, for example, a value of **5** is entered, the user's last five passwords are stored. If the value is **0**, then no passwords are stored in the password history.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3** and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted in the password. If this option is set, name properties are not permitted in passwords. The values of these columns are taken into account if the **Contains name properties for password check** option is set. In the Designer, adjust this option in the column definition. For more information, see the *One Identity Manager Configuration Guide*.

Character classes for passwords

Use the **Character classes** tab to specify which characters are permitted for a password.

Table 21: Character classes for passwords

Property	Meaning
Required number of character classes	Number of rules for character classes that must be fulfilled so that a password adheres to the password policy. The following rules are taken into account for **Min. number letters**, **Min. number lowercase**, **Min. number uppercase**, **Min. number digits**, and **Min. number special characters**. That means: • Value **0**: All character class rules must be fulfilled. • Value **>0**: Minimum number of character class rules that must be

Property	Meaning
	fulfilled. At most, the value can be the number of rules with a value **>0**. NOTE: Generated passwords are not tested for this.
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted special characters.
Max. identical characters in total	Specifies the maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Specifies the maximum number of identical character that can be repeated after each other.
Denied special characters	List of special characters that are not permitted.
Do not generate lowercase letters	Specifies whether a generated password can contain lowercase letters. This setting only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether a generated password can contain uppercase letters. This setting only applies when passwords are generated.
Do not	Specifies whether a generated password can contain digits. This setting

Property	Meaning
generate digits	only applies when passwords are generated.
Do not generate special characters	Specifies whether a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting only applies when passwords are generated.

Custom scripts for password requirements

You can implement custom scripts for testing and generating passwords if the password requirements cannot be mapped with the existing settings options. Scripts are applied in addition to the other settings.

Detailed information about this topic

- Checking passwords with a script on page 93
- Generating passwords with a script on page 94

Checking passwords with a script

You can implement a script if additional policies need to be used for checking a password that cannot be mapped with the available settings.

Syntax of check scripts

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
```

With parameters:

`policy` = password policy object

`spwd` = password to check

TIP: To use a base object, take the `Entity` property of the `PasswordPolicy` class.

Example: Script that checks a password

A password cannot start with **?** or **!** . The password cannot start with three identical characters. The script checks a given password for validity.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd
As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or
            '!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in
            password")#)
        End If
    End If
End Sub
```

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **Custom target systems > Basic configuration data > Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change main data** task.
    d. On the **Scripts** tab, enter the name of the script to be used to check a password in the **Check script** field.
    e. Save the changes.

Related topics

- Generating passwords with a script on page 94

Generating passwords with a script

You can implement a generating script if additional policies need to be used for generating a random password, which cannot be mapped with the available settings.

Syntax for generating script

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

With parameters:

`policy` = password policy object

`spwd` = generated password

TIP: To use a base object, take the `Entity` property of the `PasswordPolicy` class.

Example: Script that generates a password

In random passwords, this script replaces the invalid characters **?** and **!** at the beginning of a password with **_**.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
End Sub
```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.
2. Edit the password policy.
    a. In the Manager, select the **Custom target systems > Basic configuration data > Password policies** category.
    b. In the result list, select the password policy.
    c. Select the **Change main data** task.
    d. On the **Scripts** tab, enter the name of the script to be used to generate a password in the **Generating script** field.
    e. Save the changes.

Related topics

- Checking passwords with a script on page 93

Editing the password excluded list

You can add words to a list of restricted terms to prohibit them from being used in passwords.

NOTE: The restricted list applies globally to all password policies.

To add a term to the restricted list

1. In the Designer, select the **Base data > Security settings > Password policies** category.
2. Create a new entry with the **Object > New** menu item and enter the term you want to exclude from the list.
3. Save the changes.

Verifying passwords

When you verify a password, all the password policy settings, custom scripts, and the restricted passwords are taken into account.

To verify if a password conforms to the password policy

1. In the Manager, select the **Custom target systems > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.
3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Select the table and object to be tested in **Base object for test**.
6. Enter a password in **Enter password to test**.

   A display next to the password shows whether it is valid or not.

Testing password generation

When you generate a password, all the password policy settings, custom scripts and the restricted passwords are taken into account.

To generate a password that conforms to the password policy

1. In the Manager, select the **Custom target systems > Basic configuration data > Password policies** category.
2. In the result list, select the password policy.

3. Select the **Change main data** task.
4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Initial password for new user accounts

You can issue an initial password for a new user account in the following ways:

- When you create the user account, enter a password in the main data.
- Assign a randomly generated initial password to enter when you create user accounts.
  - In the Designer, set the **TargetSystem | UNS| Accounts | InitialRandomPassword** configuration parameter.
  - Apply target system specific password policies and define the character sets that the password must contain.
  - Specify which employee will receive the initial password by email.

Related topics

- Password policies for user accounts on page 85
- Email notifications about login data on page 97

Email notifications about login data

You can configure the login information for new user accounts to be sent by email to a specified person. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages. The mail text in a mail template is defined in several languages. This means the recipient's language can be taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

The following prerequisites must be fulfilled in order to use notifications:

1. Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.
2. In the Designer, set the **Common | MailNotification | DefaultSender** configuration parameter and enter the sender address for sending the email notifications.

3. Ensure that all employees have a default email address. Notifications are sent to this address. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.
4. Ensure that a language can be determined for all employees. Only then can they receive email notifications in their own language. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

When a randomly generated password is issued for the new user account, the initial login data for a user account is sent by email to a previously specified person.

To send initial login data by email

1. In the Designer, set the **TargetSystem | UNS | Accounts | InitialRandomPassword** configuration parameter.
2. In the Designer, set the **TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the message recipient as a value.
3. In the Designer, set the **TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** configuration parameter.

   By default, the message sent uses the mail template **Employee - new user account created**. The message contains the name of the user account.
4. In the Designer, set the **TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameter.

   By default, the message sent uses the mail template **Employee - initial password for new user account**. The message contains the initial password for the user account.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

6

Mapping custom target system objects in One Identity Manager

A custom target system's user accounts, groups, system entitlements, container structures, and additional permissions controls can be mapped in One Identity Manager. These objects are imported into the One Identity Manager database during synchronization. You cannot display or edit their properties in the Manager. To differentiate between objects from different custom target systems in the One Identity Manager database, specify an ID for each target system.

Detailed information about this topic

- Custom target system identifiers on page 99
- Container structures in custom target systems on page 105
- User accounts in custom target systems on page 106
- Groups in custom target systems on page 115
- System entitlements in custom target systems on page 119
- Reports about custom target systems on page 127

Custom target system identifiers

To differentiate between objects from different custom target systems in the One Identity Manager database, specify an ID for each target system. Each object can be assigned to exactly one target system through this ID. You can add more properties to each ID to describe the target system in more detail.

To set up custom target systems

- In the Designer, set the **TargetSystem | UNS | CreateNewRoot** configuration parameter and compile the database.

  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*.

To create or edit a target system identifier

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Target systems** category.
2. Select a target system in the result list. Select the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the target system type main data.
4. Save the changes.

TIP: You can also edit target system properties in the Manager in the **Custom Target Systems > <target system>** category.

Detailed information about this topic

- General main data for custom target systems on page 100
- Customizing data synchronization for custom target systems on page 103
- Defining categories for inheriting groups and system entitlements on page 103
- Specifying alternative column names on page 104
- Setting deferred deletion for custom target system user accounts on page 54

General main data for custom target systems

Enter the following data for a custom target system.

Table 22: Custom target system main data

Property	Description
Target system	Name of the target system.
Target system type	Type of the target system. Several target systems can be grouped together in a target system type. You can assign user accounts to groups belonging to different target systems within a target system type.
Canonical name	Name of the target system conforming with DNS syntax. `target system name.parent target system name.primary system name`

Property	Description
Distinguished name	Target system's distinguished name. This distinguished name is used to form distinguished names for child objects. If the target system does not supply any distinguished names, you can enter the target system identifier here, for example. Syntax example: `DC = <target system>`
Display name	Name that is displayed in the One Identity Manager tools for the target system.
Account definition (initial)	Initial account definition for creating user accounts. This account definition is used if automatic assignment of employees to user accounts is used for this target system and if user accounts are to be created that are already managed (**Linked configured**). The account definition's default manage level is applied. User accounts are only linked to the employee (**Linked**) if no account definition is given. This is the case on initial synchronization, for example.
Deferred deletion [days]	Number of days to defer deletion operations for this target system. For more information, see Setting deferred deletion for custom target system user accounts on page 54.
Target system managers	Application role in which target system managers are specified. The target system managers only modify the target system objects assigned to them. Therefore, each target system can have a different target system manager assigned to it. Select the One Identity Manager application role whose members are responsible for administration of this target system. Use the button to add a new application role.
Synchronized by	Type of synchronization through which the data is synchronized between the target system and One Identity Manager. You can no longer change the synchronization type once objects for this target system are present in One Identity Manager.

Table 23: Permitted values

Value	Synchronization by	Provisioned by
Synchronization by script	none	One Identity Manager script components
No synchron-ization	none	none

If you select **Scripted synchronization**, you can define custom

Property	Description
	processes to exchange data between One Identity Manager and the target system. You can configure data imports with the program Data Import or set up synchronization with the CSV connector in the Synchronization Editor.
Types of system entitlements used	Types of system entitlements to which user accounts can be assigned in this target system.
User account contains memberships	Specifies which types of system entitlements maintain assignments to user accounts. Enables the types that maintain assignments to user accounts. The assignments are saved in the `UNSAccountBHasUNSGroupB`, `UNSAccountBHasUNSGroupB1`, `UNSAccountBHasUNSGroupB2`, `UNSAccountBHasUNSGroupB3` tables. Disables the types that maintain assignments to user accounts. The assignments are saved in the `UNSAccountBInUNSGroupB`, `UNSAccountBInUNSGroupB1`, `UNSAccountBInUNSGroupB2`, `UNSAccountBInUNSGroupB3` tables. Example: In the **System entitlement types used** menu, the values **Group** and **System entitlement 1** are selected. In the **User account contains memberships** menu, only the value **System entitlement 1** is selected. Assignments to system entitlements are saved in the `UNSAccountBHasUNSGroupB1` (**System entitlement 1: assignments to user accounts**) and `UNSAccountBInUNSGroupB` (**User accounts: assignments to groups**) tables.
Description	Text field for additional explanation.
Group memberships as MVP	Specifies whether group memberships can be grouped together as a list on an multi-value property column of this target system's user accounts (relevant for data import).
Container structure	Specifies whether the target system has a contain structure.

Related topics

- Target system types for custom target systems on page 136
- Assigning employees automatically to user accounts on page 43
- Target system managers on page 133
- Specifying types of system entitlements in use on page 57

Customizing data synchronization for custom target systems

You can make special adjustments for synchronizing data between the One Identity Manager database and target system environment. The following information is displayed for a data synchronization:

Table 24: Data synchronization main data

Property	Description
synchronization server	Unique server ID. Select the server to handle the processes for the target system from the list. This synchronization server is used, for example, when provisioning is done through synchronization by script.
No write operations	Use this option to prevent changes to target system objects from the One Identity Manager database being provisioned in the target system.

Related topics

- Job server for provisioning data in a custom target system on page 13

Defining categories for inheriting groups and system entitlements

NOTE: The functionality described here for groups applies equally to system entitlements.

In One Identity Manager, user accounts can selectively inherit groups. To do this, groups and user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within the template. The mapping rule contains different tables. Use the user account table to specify categories for target system dependent user accounts. In the group table, enter your categories for the target system-dependent groups. Each table contains the category positions **position 1** to **position 63**.

Prerequisites

- Ensure that the `UNSAccountB`, `UNSGroupB`, and `UNSRootB` tables are assigned to the target system type. For more information, see Adding custom tables to the target system synchronization on page 18.

To assign tables to the target system type

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Target system types** category.
2. In the result list, select the target system type of the customer target system.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the `UNSAccountB`, `UNSGroupB`, and `UNSRootB` tables.
    - If used, assign the `UNSGroupB1`, `UNSGroupB2`, and `UNSGroupB3` tables.
5. Save the changes.

To define a category

1. In the Manager, select the target system in the **Custom target systems** category.
2. Select the **Change main data** task.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of a table.
5. To enable the category, double-click .
6. Enter a category name of your choice for user accounts and groups in the login language that you use.
7. Save the changes.

Detailed information about this topic

- Inheriting groups and system entitlements based on categories on page 81

Specifying alternative column names

If you require different names for input fields to those on the main data form, you can specify a language-dependent alternative column name for each object type.

To specify alternative column names

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Target systems** category.
2. In the result list, select a target system and run the **Change main data** task.
3. Switch to the **Alternative column names** tab.
4. Open the membership tree in the table whose column name you want to change.

   All the columns in this table are listed with their default column names.
5. Enter any name in the login language in use.
6. Save the changes.

Container structures in custom target systems

The container structure represents the structure elements of a target system. Containers are represented by a hierarchical tree structure.

To edit or create a container

1. In the Manager, select the **Custom Target Systems > <target system> > Container structure** category.
2. Select the container in the result list and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the container's main data.
4. Save the changes.

Detailed information about this topic

- Main data for containers on page 105

Main data for containers

Enter the following main data of a container.

Table 25: Main data for a container

Property	Description
Target system	Name of the target system.
Name	Container name.
Canonical name	Canonical name of the container. The canonical name is generated automatically and should not be changed.
Distinguished name	Container's distinguished name. The distinguished name is determined using a template and must not be changed.
Object GUID	Unique ID used for managing the object in the target system.
Parent container	Parent container for mapping a hierarchical container structure. The distinguished name is automatically updated using templates.
Description	Text field for additional explanation.

User accounts in custom target systems

User accounts represent a target system's authentication objects. A user account obtains the required permissions for accessing target system resources through its memberships in groups and system entitlements.

A user account can be linked to an employee in One Identity Manager. You can also manage user accounts separately from employees.

NOTE: It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the main data described in the following is mapped through templates from employee main data.

NOTE: If employees are to obtain their user accounts through account definitions, the employees must own a central user account and obtain their IT operating data through assignment to a primary department, a primary location, or a primary cost center.

Related topics

- Managing user accounts and employees on page 21
- Account definitions for user accounts on page 22
- Managing assignments of groups and system entitlements on page 57
- Creating and editing user accounts on page 106
- User account main data on page 107
- Assigning extended properties to user accounts on page 111
- Assigning permissions controls to user accounts on page 112
- Disabling user accounts on page 112
- Deleting and restoring user accounts on page 114
- Displaying the user account overview on page 115

Creating and editing user accounts

A user account can be linked to an employee in One Identity Manager. You can also manage user accounts separately from employees.

NOTE: It is recommended to use account definitions to set up user accounts for company employees. In this case, some of the main data described in the following is mapped through templates from employee main data.

To create a user account

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Click in the result list.

3. On the main data form, edit the main data of the user account.
4. Save the changes.

To edit main data of a user account

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Edit the user account's resource data.
5. Save the changes.

To manually assign a user account for an employee

1. In the Manager, select the **Employees > Employees** category.
2. Select the employee in the result list.
3. Select the **Assign user accounts** task.
4. Assign a user account.
5. Save the changes.

Related topics

- User account main data on page 107
- Managing user accounts and employees on page 21
- Supported user account types on page 48
- Account definitions for user accounts on page 22

User account main data

Enter the following data for a user account:

Table 26: User account properties

Property	Description
Employee	Employee that uses this user account. An employee is already entered if the user account was generated by an account definition. If you create the user account manually, you can select an employee in the menu. You can create a new employee for a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity**, or **Service identity**. To do this, click next to the input field and enter the required employee main data. Which login data is required depends on the

Property	Description
	selected identity type.
No link to an employee required	Specifies whether the user account is intentionally not assigned an employee. The option is automatically set if a user account is included in the exclusion list for automatic employee assignment or a corresponding attestation is carried out. You can set the option manually. Enable the option if the user account does not need to be linked with an employee (for example, if several employees use the user account). If attestation approves these user accounts, these user accounts will not be submitted for attestation in the future. In the Web Portal, user accounts that are not linked to an employee can be filtered according to various criteria.
Not linked to an employee	Indicates why the **No link to an employee required** option is enabled for this user account. Possible values: • **By administrator**: The option was set manually by the administrator. • **By attestation**: The user account was attested. • **By exclusion criterion**: The user account is not associated with an employee due to an exclusion criterion. For example, the user account is included in the exclude list for automatic employee assignment (configuration parameter **PersonExcludeList**).
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account main data and to specify a manage level for the user account. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved. NOTE: Use the user account's **Remove account definition** task to reset the user account to **Linked** status. This removes the account definition from both the user account and the employee. The user account remains but is not managed by the account definition anymore. The task only removes account definitions that are directly assigned (`XOrigin=1`).
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Target system	Name of the target system.

Property	Description
First name	The user's first name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Last name	The user's last name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Container	Container in which to create the user account. If you have assigned an account definition, the container is determined from the company IT data for the assigned employee depending on the manage level of the user account. When the container is selected, the defined name for the user is created using a formatting rule.
Login name	Name the user uses to log onto the target system. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Name	User account identifier. The identifier is made up of the user's first and last names.
Canonical name	Canonical name of the user account. The canonical name is generated automatically and should not be changed.
Distinguished name	User account's distinguished name. The distinguished name is determined using a template and must not be changed.
Object GUID	Unique ID used for managing the object in the target system.
Display name	User account display name.
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Account expiry date	The date up to which the user can log into a target system with this user account. If a leaving date is specified for an employee, this date is used as the account expiration date depending on the manage level. Any existing account expiry date is overwritten in this case. NOTE: If the employee's leaving date is deleted at a later point in time, the user account expiration date remains intact.
Last login	Date of last target system login.
Password	Password for the user account. The employee's central password can be

Property	Description
	mapped to the user account password. For more information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*. If you use a random generated initial password for the user accounts, it is automatically entered when a user account is created. The password is deleted from the database after publishing to the target system. NOTE: One Identity Manager password policies are taken into account when a user password is being verified. Ensure that the password policy does not violate the target system's requirements.
Password confirmation	Reconfirm password.
Password last changed	Data of last password change.
Description	Text field for additional explanation.
Identity	User account's identity type Permitted values are: • **Primary identity**: Employee's default user account. • **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • **Personalized administrator identity**: User account with administrative permissions, used by one employee. • **Sponsored identity**: User account to use for a specific purpose. Training, for example. • **Shared identity**: User account with administrative permissions, used by several employees. Assign all employees that use this user account. • **Service identity**: Service account.
Privileged user account.	Specifies whether this is a privileged user account.
Groups can be inherited	Specifies whether the user account can inherit groups through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.

Property	Description
	• If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
System entitlements 1 can be inherited System entitlements 2 can be inherited System entitlements 3 can be inherited	Specifies whether the user account may inherit system entitlements of the corresponding type through the linked employee. If the option is set, the user account inherits groups through hierarchical roles, in which the employee is a member, or through IT Shop requests. • For example, if you add an employee with a user account to a department and you have assigned system entitlements to that department, the user account inherits those system entitlements. • If an employee has requested an assignment to a system entitlement in the IT Shop and this request is approved and assigned, then the employee's user account inherits this system entitlement only if the option is enabled.
User account is disabled	Specifies whether the user account is locked. If a user account is not required for a period of time, you can temporarily disable the user account by using the <User account is deactivated> option.

Related topics

- Account definitions for user accounts on page 22
- Assigning employees automatically to user accounts on page 43
- Password policies for user accounts on page 85
- Initial password for new user accounts on page 97
- Supported user account types on page 48
- Inheriting groups and system entitlements based on categories on page 81
- Prerequisites for indirect assignments of groups and system entitlements to user accounts on page 61
- Disabling user accounts on page 112
- General main data for custom target systems on page 100

Assigning extended properties to user accounts

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 using extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To specify extended properties for a user account

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Select **Assign extended properties**.
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.

Assigning permissions controls to user accounts

Use this task to assign multiple permissions controls to a user account.

To assign permissions controls to a user account

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Select **Assign permissions controls**.
4. In the **Add assignments** pane, assign permissions controls.

   TIP: In the **Remove Assignments** pane, you can remove the assigned permission controls.

   To remove an assignment

   - Select the permissions control and double-click .
5. Save the changes.

Related topics

- Assigning user accounts to permissions controls on page 125

Disabling user accounts

The way you disable user accounts depends on how they are managed.

Scenario: User accounts are linked to employees and are managed through account definitions.

User accounts managed through account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. Accounts with the **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the `UNSAccountB.AccountDisabled` column.

Scenario: The user accounts are linked to employees. No account definition is applied.

User accounts managed through user account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the **QER | Person | TemporaryDeactivation** configuration parameter

- If the configuration parameter is set, the employee's user accounts are disabled when the employee is permanently or temporarily disabled.
- If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.

To the user account when the configuration parameter is disabled

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

Scenario: The user accounts are not linked to employees.

To disable a user account that is no longer linked to an employee

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. On the **General** tab, set the **Account is disabled** option.
5. Save the changes.

For more information about deactivating and deleting employees and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

Related topics

- Deleting and restoring user accounts on page 114
- Creating account definitions on page 23
- Creating manage levels on page 27

Deleting and restoring user accounts

NOTE: As long as an account definition for an employee is valid, the employee retains the user account that was created by it. If the account definition assignment is removed, the user account that was created from this account definition, is deleted.

You can delete a user account that was not created using an account definition through the result list or from the menu bar. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager. The user account is locked in One Identity Manager and permanently deleted from the One Identity Manager database and the target system depending on the deferred deletion setting.

For more information about deactivating and deleting employees and user accounts, see the *One Identity Manager Target System Base Module Administration Guide*.

To delete a user account that is not managed using an account definition

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Click in the result list.
4. Confirm the security prompt with **Yes**.

To restore a user account

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Click in the result list.

Related topics

- Disabling user accounts on page 112
- Setting deferred deletion for custom target system user accounts on page 54

Displaying the user account overview

Use this task to obtain an overview of the most important information about a user account.

To obtain an overview of a user account

1. In the Manager, select the **Custom Target Systems > <target system> > User accounts** category.
2. Select the user account in the result list.
3. Select the **User account overview** task.

Groups in custom target systems

Groups and system entitlements represent the objects used in the target system to control access to target system resources. A user account obtains the required permissions for accessing target system resources through its memberships in groups and system entitlements.

To create a group

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Click in the result list.
3. On the main data form, edit the main data of the group.
4. Save the changes.

To edit group main data

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the main data of the group.
5. Save the changes.

Related topics

- Managing assignments of groups and system entitlements on page 57
- System entitlements in custom target systems on page 119
- Main data for groups on page 116
- Assigning groups to groups on page 117

- Assigning permissions controls to groups on page 118
- Assigning extended properties to groups on page 118
- Displaying the group overview on page 119

Main data for groups

Enter the following main data of a group.

Table 27: Entering main data of a group

Property	Description
Name	Name of the group.
Canonical name	The canonical name is generated automatically and should not be changed.
Group type	Detailed name of the group type.
Distinguished name	The distinguished name is determined using a template and must not be changed.
Object GUID	Unique ID used for managing the object in the target system.
Display name	Name for displaying the group in the user interface of One Identity Manager tools.
Target system	Name of the target system.
Container	Container in which to create the group.
Service item	Service item data for requesting the group through the IT Shop.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Set a value in the range **0** to **1**. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated. For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups and user accounts are divided into categories. Select one or more categories from the menu.
Description	Text field for additional explanation.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in	Specifies whether the group can only be requested through the IT Shop.

Property	Description
IT Shop	If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is not permitted.
Read-only memberships	Specifies whether memberships are read-only. For example, dynamic groups. The memberships are regulated by the target system. Manual changes to memberships in One Identity Manager are not permitted.

Related topics

- Inheriting groups and system entitlements based on categories on page 81
- Adding groups to the IT Shop on page 70

Assigning groups to groups

Use this task to add a group to another group. This means that the groups can be hierarchically structured. Only groups from the same target system can be assigned.

To assign groups directly to a group as members

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** category.
4. Select the **Has members** tab.
5. Assign child groups in **Add assignments**.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click .
6. Save the changes.

To add a group as a member of other groups

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** task.
4. Select the **Is member of** tab.

5. In the **Add assignments** pane, assign parent groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.

6. Save the changes.

Related topics

- Assigning system entitlements to system entitlements on page 122

Assigning extended properties to groups

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 setting up extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To specify extended properties for a group

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select **Assign extended properties**.
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.

Related topics

- Assigning extended properties to system entitlements on page 123

Assigning permissions controls to groups

Use this task to assign multiple permissions controls to a group.

To assign permissions controls to a group

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign permissions controls** task.
4. In the **Add assignments** pane, assign permissions controls.

   TIP: In the **Remove Assignments** pane, you can remove the assigned permission controls.

   To remove an assignment

   - Select the permissions control and double-click .
5. Save the changes.

Related topics

- Assigning groups to permissions controls on page 126

Displaying the group overview

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

To obtain an overview of a group

1. In the Manager, select the **Custom Target Systems > <target system> > Groups** category.
2. Select the group in the result list.
3. Select the **Group overview** task.

System entitlements in custom target systems

Groups and system entitlements represent the objects used in the target system to control access to target system resources. A user account obtains the required permissions for accessing target system resources through its memberships in groups and system entitlements.

To create a system entitlement

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.
2. Click in the result list.
3. On the main data form, edit the system entitlement's main data.
4. Save the changes.

To edit the main data of a system entitlement:

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **Change main data** task.
4. On the main data form, edit the system entitlement's main data.
5. Save the changes.

Related topics

- Managing assignments of groups and system entitlements on page 57
- Groups in custom target systems on page 115
- System entitlement main data on page 120
- Assigning system entitlements to system entitlements on page 122
- Assigning extended properties to system entitlements on page 123
- Displaying system entitlement overviews on page 124

System entitlement main data

Enter the following main data for a system entitlement.

Table 28: General main data of a system entitlement

Property	Description
Name	Name of the system entitlement.
Canonical name	The canonical name is generated automatically and should not be changed.
System entitlement type	Details of the system entitlement type.
Distinguished name	The distinguished name is determined using a template and must not be changed.
Object GUID	Unique ID used for managing the object in the target system.
Display name	The display name is used to display the system entitlement in the One Identity Manager tools' user interface.
Target system	Name of the target system.
Container	Container in which the system entitlement is added.
Service item	Service item for requesting the system entitlement through the IT Shop.
Risk index	Value for evaluating the risk of assigning the system entitlement to user accounts. Set a value in the range **0** to **1**. 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*.
Category	Category for inheriting system entitlements. User accounts can inherit system entitlements selectively. To do this, system entitlements and user accounts are divided into categories. Select one or more categories from the menu.
Description	Text field for additional explanation.
IT Shop	Specifies whether the system entitlement can be requested through the IT Shop. If this option is set, the system entitlement can be requested by the employees through the Web Portal and distributed with a defined approval process. The system entitlement can still be assigned directly to user accounts and hierarchical roles.
Only for use in IT Shop	Specifies whether the system entitlement can only be requested through the IT Shop. If this option is set, the system entitlement can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the system entitlement to hierarchical roles or user accounts is not permitted.
Read-only memberships	Specifies whether memberships are read-only. For example, dynamic groups. The memberships are regulated by the target system. Manual changes to memberships in One Identity Manager are not permitted.

Related topics

- Inheriting groups and system entitlements based on categories on page 81
- Adding system entitlements to the IT Shop on page 71

Assigning system entitlements to system entitlements

System entitlements can be members of other system entitlements. This means that the system entitlements can be hierarchically structured. You can only assign system entitlements of the same type and the same target system.

To assign system entitlements as members to a system entitlement

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **System entitlements 1 overview** task, **System entitlements 2 overview** task, or **System entitlements 3 overview** task to match the selected system entitlement.
4. Select the **Has members** tab.
5. In the **Add assignments** pane, assign the child system entitlements.

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

   To remove an assignment

   - Select the system entitlement and double-click .
6. Save the changes.

To add a system entitlement as a member to another system entitlement

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

- OR -

In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.

2. Select the system entitlement in the result list.
3. Select the **System entitlements 1 overview** task, **System entitlements 2 overview** task, or **System entitlements 3 overview** task to match the selected system entitlement.
4. Select the **Is member of** tab.
5. In the **Add assignments** pane, assign the parent system entitlements.

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

   To remove an assignment

   - Select the system entitlement and double-click ✓.
6. Save the changes.

Related topics

- Assigning groups to groups on page 117

Assigning extended properties to system entitlements

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 setting up extended properties, see the *One Identity Manager Identity Management Base Module Administration Guide*.

To specify extended properties for a system entitlement

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.

3. Select **Assign extended properties**.
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.

Related topics

- Assigning extended properties to groups on page 118

Displaying system entitlement overviews

You use this task to obtain an overview of the most important information about a system entitlement.

To obtain an overview of a system entitlement

1. In the Manager, select the **Custom Target Systems > <target system> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Custom Target Systems > <target system> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **System entitlement 1 overview** task, **System entitlement 2 overview** task, or **System entitlement 3 overview** task to match the selected system entitlement.

Permissions controls in custom target systems

Use permissions controls to map more properties of the target systems. To do this, you can import the data you want into One Identity Manager from the connected target system. You can also add permissions controls in One Identity Manager.

To edit permissions controls

1. In the Manager, select the **Custom Target Systems > <target system> > Permissions controls** category.
2. Select a permissions control in the result list. Select the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the permissions controls' main data.
4. Save the changes.

Detailed information about this topic

- Main data for permissions controls on page 125
- Assigning groups to permissions controls on page 126
- Assigning user accounts to permissions controls on page 125
- Displaying the permissions control overview on page 127

Main data for permissions controls

Enter the following main data of a permissions control.

Table 29: Permissions control main data

Property	Description
Target system	Target system in which the permissions control applies.
Permissions control	Name of the permissions control.
Permissions type	Additional permissions control properties.
Description	Text field for additional explanation.
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.

Assigning user accounts to permissions controls

Use this task to assign a permissions control to multiple user accounts.

To assign permissions controls to user accounts

1. In the Manager, select the **Custom Target Systems > <target system> > Permissions controls** category.
2. Select the permissions control in the result list.
3. Select the **Assign user accounts** task.
4. In the **Add assignments** pane, assign the user accounts.

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

   To remove an assignment

   - Select the user account and double-click ✓.
5. Save the changes.

Related topics

- Assigning permissions controls to user accounts on page 112

Assigning groups to permissions controls

Use this task to assign a permissions control directly to multiple groups.

To assign groups to a permissions control

1. In the Manager, select the **Custom Target Systems > <target system> > Permissions controls** category.
2. Select the permissions control in the result list.
3. Select **Assign groups** category.
4. In the **Add assignments** pane, assign the groups.

   TIP: In the **Remove assignments** pane, you can remove the assignment of groups.

   To remove an assignment

   - Select the group and double-click ✓.
5. Save the changes.

Related topics

- Assigning permissions controls to groups on page 118

Displaying the permissions control overview

You can see the most important information about a permissions control on the overview form.

To obtain an overview of a permissions control

1. In the Manager, select the **Custom Target Systems > <target system> > Permissions controls** category.
2. Select the permissions control in the result list.
3. Select the **Permissions control overview** task.

Reports about custom target systems

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 custom target systems.

NOTE: Other sections may be available depending on the which modules are installed.

Table 30: Data quality target system report

Report	Published for	Description
Show overview	User account	This report shows an overview of the user account and the assigned permissions.
Show overview including origin	User account	This report shows an overview of the user account and origin of the assigned permissions.
Show overview including history	User account	This report shows an overview of the user accounts including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts overview (incl. history)	Container	This report shows all the container's user accounts with their permissions including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.

Report	Published for	Description
Show system entitlements overview (incl. history)	Container	This report shows the container's system entitlements with the assigned user accounts including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Container	This report finds all roles containing employees with at least one user account in the selected container.
Overview of all assignments	System entitlement group	This report finds all roles containing employees who have the selected system entitlement.
Show overview	System entitlement group	This report shows an overview of the system entitlement and its assignments.
Show overview including origin	System entitlement group	This report shows an overview of the system entitlement and origin of the assigned user accounts.
Show overview including history	System entitlement group	This report shows an overview of the system entitlement and including its history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show entitlement drifts	Target system	This report shows all system entitlements that are the result of manual operations in the target system rather than provisioned by One Identity Manager.
Show user accounts overview (incl. history)	Target system	This report returns all the user accounts with their permissions including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Show user accounts with an above average	Target system	This report contains all user accounts with an above average number of system entitlements.

Report	Published for	Description
number of system entitlements		
Show employees with multiple user accounts	Target system	This report shows all the employees that have multiple user accounts. The report contains a risk assessment.
Show system entitlements overview (incl. history)	Target system	This report shows the system entitlements with the assigned user accounts including a history. Select the end date for displaying the history (**Min. date**). Older changes and assignments that were removed before this date, are not shown in the report.
Overview of all assignments	Target system	This report finds all roles containing employees with at least one user account in the selected target system.
Show unused user accounts	Target system	This report contains all user accounts, which have not been used in the last few months.
Show orphaned user accounts	Target system	This report shows all user accounts to which no employee is assigned.
Show user account operations	Target system	This report shows modified user accounts from all target systems for a specific time period.

Related topics

- Overview of all assignments on page 83

Treatment of custom target system objects in the Web Portal

One Identity Manager enables its users to perform various tasks simply using a Web Portal.

- Managing user accounts and employees

  An account definition can be requested by shop customers in the Web Portal if it is assigned to an IT Shop shelf. The request undergoes a defined approval process. The user account is not created until it has been agreed by an authorized person, such as a manager.

- Managing assignments of groups and system entitlements

  These products can be requested in the Web Portal by the shop's customers by assigning groups and system entitlements to an IT Shop shelf. The request undergoes a defined approval process. The group or system entitlement is not assigned until it has been approved by an authorized person.

  In the Web Portal, managers and administrators of organizations can assign system entitlements to the departments, cost centers, or locations for which they are responsible. The system entitlements and groups are inherited by all employees who are members of these departments, cost centers, or locations.

  If the Business Roles Module is available, managers and administrators of business roles can assign groups and system entitlements to the business roles in the Web Portal for which they are responsible. The groups and system entitlements are inherited by all employees who are members of these business roles.

  If the System Roles Module is available, those with system roles responsibilities can assign groups and system entitlements to the system roles in the Web Portal. The groups and system entitlements are inherited by all employees to whom these system roles are assigned.

- Attestation

  If the Attestation Module is available, the correctness of the properties of target system objects and of entitlement assignments can be verified on request. To enable this, attestation policies are configured in the Manager. The attestors use the Web Portal to approve attestation cases.

- Governance administration

  The rules are checked regularly, and if changes are made to the objects in One Identity Manager. Compliance rules are defined in the Manager. Supervisors use the Web Portal to check and resolve rule violations and to grant exception approvals.

  If the Company Policies Module is available, company policies can be defined for the target system objects mapped in One Identity Manager and their risks evaluated. Company policies are defined in the Manager. Supervisors use the Web Portal to check policy violations and to grant exception approvals.

- Risk assessment

  You can use the risk index of groups to evaluate the risk of entitlement assignments for the company.One Identity Manager provides default calculation functions for this. The calculation functions can be modified in the Web Portal.

- Reports and statistics

  The Web Portal provides a range of reports and statistics about the employees, user accounts, and their entitlements and risks.

For more information about the named topics, see Managing user accounts and employees on page 21, Managing assignments of groups and system entitlements on page 57, and the following guides:

- *One Identity Manager Web Designer Web Portal User Guide*
- *One Identity Manager Attestation Administration Guide*
- *One Identity Manager Compliance Rules Administration Guide*
- *One Identity Manager Company Policies Administration Guide*
- *One Identity Manager Risk Assessment Administration Guide*

8

Basic configuration data for custom target systems

The following base data is relevant for managing a custom target system in One Identity Manager.

- Account definitions

  One Identity Manager has account definitions for automatically allocating user accounts to employees. You can create account definitions for every target system. If an employee does not yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

  For more information, see Account definitions for user accounts on page 22.

- Password policy

  One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

  Predefined password policies are supplied with the default installation that you can use or customize if required. You can also define your own password policies.

  For more information, see Password policies for user accounts on page 85.

- Initial password for new user accounts

  You have the different options for issuing an initial password for user accounts. Enter a password or use a random generated initial password when you create a user account.

  For more information, see Initial password for new user accounts on page 97.

- Email notifications about credentials

  When a new user account is created, the login data are sent to a specified recipient. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages.

  For more information, see Email notifications about login data on page 97.

- Server

A server on which One Identity Manager Service is installed configured and started must be provided to provision data from One Identity Manager into a custom target system using synchronization by script. The server must be declared in One Identity Manager and entered as the synchronization server in the target system.

For more information, see Job server for provisioning data in a custom target system on page 13.

- Target system managers

  A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who have permission to edit all target systems in One Identity Manager.

  Define additional application roles if you want to limit the permissions for target system managers to individual target systems. The application roles must be added under the default application role.

  For more information, see Target system managers on page 133.

- Target system types

  Several target systems can be grouped together in a target system type. Depending on the configuration of the target system type, groups and system entitlements can also be assigned to user accounts even if they belong to different target systems. Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

  For more information, see Target system types for custom target systems on page 136.

- Custom schema extensions to base tables

  You can display custom columns of the `UNSAccountB`, `UNSContainerB`, `UNSGroupB`, `UNSGroupB1`, `UNSGroupB2`, `UNSGroupB3`, `UNSItemB`, and `UNSRootB` tables on the forms in the Manager. To do this, modify the custom column's column definition.

  For more information, see Configuring display of custom schema extensions for custom target systems on page 137.

Target system managers

A default application role exists for the target system manager in One Identity Manager. Assign employees to this application role who have permission to edit all target systems in One Identity Manager.

Define additional application roles if you want to limit the permissions for target system managers to individual target systems. The application roles must be added under the default application role.

For more information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Implementing application roles for target system managers

1. The One Identity Manager administrator allocates employees to be target system administrators.
2. These target system administrators add employees to the default application role for target system managers.

   Target system managers with the default application role are authorized to edit all the target systems in One Identity Manager.
3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual target systems.

Table 31: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | Custom target systems** application role or a child application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change, or delete target system objects. • Edit password policies for the target system. • Prepare groups and system entitlements to add to the IT Shop. • Can add employees who have another identity than the **Primary identity**. • Configure synchronization in the Synchronization Editor and define the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

1. Log in to the Manager as a One Identity Manager administrator (**Base role \| Administrators** application role)
2. Select the **One Identity Manager Administration > Target systems > Administrators** category.
3. Select the **Assign employees** task.
4. Assign the employee you want and save the changes.

To add the first employees to the default application as target system managers

1. Log in to the Manager as a target system administrator (**Target systems | Administrators** application role).
2. Select the **One Identity Manager Administration > Target systems > Custom target systems** category.
3. Select the **Assign employees** task.
4. Assign the employees you want and save the changes.

To authorize other employees as target system managers when you are a target system manager

1. Log in to the Manager as a target system manager.
2. Select the application role in the **Custom Target Systems > Basic configuration data > Target system managers** category.
3. Select the **Assign employees** task.
4. Assign the employees you want and save the changes.

To specify target system managers for individual target systems

1. Log in to the Manager as a target system manager.
2. Select the **Custom Target Systems > Basic configuration data > Target systems** category.
3. Select the **Change main data** task.
4. On the **General** tab, select the application role in the **Target system manager** menu.

   - OR -

   Next to the **Target system manager** menu, click to create a new application role.

   a. Enter the application role name and assign the **Target systems | Custom target systems** parent application role.

   b. Click **OK** to add the new application role.
5. Save the changes.
6. Assign employees to this application role who are permitted to edit the target system in One Identity Manager.

Related topics

- One Identity Manager users for managing custom target systems on page 8
- General main data for custom target systems on page 100

Target system types for custom target systems

Several target systems can be grouped together in a target system type. Depending on the configuration of the target system type, groups and system entitlements can also be assigned to user accounts even if they belong to different target systems. Target system types are required for configuring target system comparisons. Tables with outstanding objects are maintained with the target system types and settings are configured for provisioning memberships and single objects synchronization. Target system types also map objects in the Unified Namespace.

To create or edit a target system type

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Target system types** category.
2. In the result list, select the target system type.

   - OR -

   Click in the result list.
3. Edit the target system type main data.

Table 32: main data for a target system type

Property	Description
Target system type	Target system type description.
Description	Text field for additional explanation.
Display name	Name of the target system type as displayed in One Identity Manager tools.
Cross-boundary inheritance	Specifies how user accounts are assigned to or inherit groups and system entitlements if they belong to different custom target systems. • If the option is set, groups and system entitlements can be assigned to user accounts that belong to the same target system or to different target systems. The target systems must have the same target system type. For all target systems of a target system type, the settings for the **User Account Contains Memberships** column (`UNSRootB.UserContainsGroupList`) must be identical. • If the option is not set, groups and system entitlements can only be assigned to the same target system. NOTE: If the option is not set, the target system type is used to

Property	Description
	simplify grouping of the target systems.
Show in compliance rule wizard	Specifies whether the target system type for compliance rule wizard can be selected when rule conditions are being set up.
Text snippet	Text snippets used for linking text in the compliance rule wizard.
Alternative connectors	List of connector that can process this type of target system.

4. Save the changes.

To assign a custom target system to a target system type

1. In the Manager, select the **Custom Target Systems > Basic configuration data > Target systems** category.
2. Select the target system in the result list.
3. Select the **Change main data** task.
4. From the **Target system type** menu, select the target system type to which you want to assign the target system.
5. Save the changes.

Related topics

- Assigning groups and system entitlements to user accounts in One Identity Manager on page 60
- Post-processing outstanding objects on page 17
- Adding custom tables to the target system synchronization on page 18

Configuring display of custom schema extensions for custom target systems

You can display custom columns of the `UNSAccountB`, `UNSContainerB`, `UNSGroupB`, `UNSGroupB1`, `UNSGroupB2`, `UNSGroupB3`, `UNSItemB`, and `UNSRootB` tables on the forms in the Manager. To do this, modify the custom column's column definition.

For more information about adding custom columns to tables using the Schema Extension program and adjusting the column definitions using the Designer, see the *One Identity Manager Configuration Guide*.

To display custom columns of the UNSAccountB, UNSContainerB, UNSGroupB, UNSGroupB1, UNSGroupB2, UNSGroupB3, UNSItemB, and UNSRootB tables on forms in the Manager

- In the Designer, specify the order for displaying input fields in the **Sort order** property (`DialogColumn.SortOrder`). Columns with a sort order of less that one are not displayed.
- In the Designer, modify the **Group** property (`DialogColumn.ColumnGroup`) in the column definition of the custom columns. The group determines which tab the column will appear on.
    - If you do not enter a group in the column configuration, the column will be displayed on a tab with the name **Custom** for all target system types.
    - If you enter a group in the column configuration, the column will be displayed on a tab with the group's name for all target system types. The group's name must not match the name of a target system type.
    - If you want to display a column for a particular target system type, only enter the specific target system type (`DPRNamespace.Ident_DPRNamespace`) as group. The column is displayed on a tab with the target system type's name. The column is not displayed for any other target system types.
    - To display more than one target system type, enter the target system types as groups by delimiting them with a comma. The column will be displayed on a tab with the target system type's name for each of the target system types entered. The column is not displayed for any other target system types.
    - To display the column for one or more target system types, but only on one tab with another name, enter the target system types delimited by commas (,) and the tab name as the group. This group will be used as tab name for all the target system types entered. The column is not displayed for any other target system types.

Example:

`UNSAccountB` is extended by five columns. The columns should be displayed as follows for target system type A, target system type B and target system type C.

- You want to display Column 1 on the **Custom** tab for all target system types.
- You want to display Column 2 on the **Group A** tab for all target system types.
- You want to display Column 3 on the **Target system type B** tab for target system type B. Columns are not displayed for target system type A and target system type C.
- You want to display column 4 for target system type B on the **Target system type B** tab and for target system type C on the **Target system type C** tab. The column is not displayed for target system type A.

- You want to display Column 5 on the **Group A** tab for target system type B and target system type C. The column is not displayed for target system type A.

Table 33: Column configuration example

Column	Group
Column 1	
Column 2	Group A
Column 3	Target system type B
Column 4	Target system type B, target system type C
Column 5	Target system type B, target system type C, group A

Appendix A

Configuration parameters for managing custom target systems

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

Table 34: Configuration parameters for managing custom target systems

Configuration parameters	Meaning
TargetSystem | UNS	General configuration parameter for managing custom target systems.
TargetSystem | UNS | Accounts	Allows configuration of user account data.
TargetSystem | UNS | Accounts | InitialRandomPassword	Specifies whether a random password is generated when new user accounts are added. It must contain at least those character sets set in the configuration subparameters.
TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo	Employee to receive an email with the random generated password (manager cost center/department/location/business role, employee's manager or `XUserInserted`). If no recipient can be found, the password is sent to the address stored in the configuration parameter **TargetSystem | UNS | DefaultAddress**.
TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The **Employee - new user account created** mail template is used.
TargetSystem | UNS | Accounts | InitialRandomPassword | SendTo |	Mail template name that is sent to supply users with the initial password. The **Employee - initial password for new user account** mail template is used.

Configuration parameters	Meaning
MailTemplatePassword	
TargetSystem | UNS | Accounts | MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The **Employee - new user account with default properties created** mail template is used.
TargetSystem | UNS | CreateNewRoot	Specifies whether new target systems can be created. If this parameter is set, custom target systems can be added. Changes to this parameter require the database to be recompiled. 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*.
TargetSystem | UNS | DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem | UNS | MaxFullsyncDuration	Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem | UNS | PersonAutoDefault	Mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem | UNS | PersonAutoDisabledAccounts	Specifies whether employees are automatically assigned to disabled user accounts. User accounts do not obtain an account definition.
TargetSystem | UNS | PersonAutoFullSync	Mode for automatic employee assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem | UNS | PersonExcludeList	Listing of all user account without automatic employee assignment. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $`

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

A

account definition 22
- add to IT Shop 37
- assign to system roles 37
- assign to user account 48
- edit 23
- manage level 26

C

configuration parameter 140
custom target system 7
- account definition 22
  - assign automatically 36
  - assign to all employees 36
  - assign to business role 35
  - assign to cost center 34
  - assign to department 34
  - assign to employee 33, 36
  - assign to location 34
  - create 23
  - delete 40
  - IT operating data 30-31
  - manage level 27
- container 105
- group 115
  - assign extended properties 118
  - assign group 117
  - assign permissions element 118
  - assign system role 68
  - assign to business role 65
  - assign to cost center 62
  - assign to department 62
  - assign to location 62
  - assign to user account 60, 74, 76
  - category 81, 116
  - edit 116
  - effective 78
  - exclusion 78
  - pass down 60, 81
  - risk index 116
  - target system type 136
permissions control 124
- assign group 118, 126
- assign user account 112, 125
provisioning by script 11-12
- server 13
report 127
system entitlement 119
- assign extended properties 123
- assign system entitlements 122
- assign system role 68
- assign to business role 66
- assign to user account 60, 75
- category 120
- edit 120
- effective 78
- exclusion 78
- pass down 60
- risk index 120
- save member 57
- type 57

system entitlements
assign to cost center 64
assign to department 64
assign to location 64
assign to user account 77
category 81
pass down 81
target system
account definition 40, 100
alternative column description 104
category 103
deferred deletion 54, 100
display name 100
edit 99
no write operations 103
synchronization by script 100
synchronization server 13, 103
synchronized by 100
target system managers 100
target system type 100
target system administrator 8
target system manager 8, 100, 133
target system type 136
cross boundary inheritance 136
group membership 136
user 8
user account 106
account definition 107
assign employee 21, 43
assign extended properties 111
assign group 76
assign permissions control 112
assign system entitlements 77
category 81, 107
deactivate 112
delete 114
edit 106
identity 107
inherit group 107
login name 107
manage level 47, 107
password 107
initial 97
privileged user account 107
restore 114

D

default user accounts 50

E

email notification 97
employee assignment
automatic 43
manual 46
remove 46
search criteria 45
table column 45

I

identity 48
IT operating data
change 32
IT Shop shelf
assign account definition 37

L

login data 97

N

notification 97

O

object
delete immediately 19
outstanding 17, 19
publish 19
outstanding object 17

P

password
initial 97
password policy 85
assign 87
character sets 91
check password 96
conversion script 93-94
default policy 87, 89
display name 89
edit 88-89
error message 89
excluded list 96
failed logins 90
generate password 96
initial password 90
name components 90
password age 90
password cycle 90
password length 90
password strength 90
predefined 86
test script 93

T

target system
overview of all assignments 83
target system synchronization
table to assign 18
target system type 18
template
IT operating data, modify 32

U

user account
administrative user account 51-52
apply template 32
connected 48
default user accounts 50
identity 48
password
notification 97
privileged user account 48, 53
type 48, 50, 53