One Identity Manager 8.0.1

Administration Guide for Connecting to Custom Target Systems

Copyright 2018 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 HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity make 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 do not make any commitment to update the information contained in this document.

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

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

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

Patents

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

Trademarks

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

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

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

One Identity Manager Administration Guide for Connecting to Custom Target Systems
Updated - March 2018
Version - 8.0.1

Contents

Managing Custom Target Systems **6**
One Identity Manager Users for Managing Custom Target Systems 6

Setting up Script Controlled Data Provisioning in a Custom Target System .. **9**
Creating the Script for Data Provisioning in a Custom Target System 10
Setting up a Server for Data Provisioning in a Custom Target System 11
Master Data for a Job Server 11
Specifying Server Functions 13
Post-Processing Outstanding Objects 15
Configuring Target System Synchronization 16
Post-Processing Outstanding Objects 16

Base Data for Custom Target Systems **19**
Setting Up Account Definitions 20
Creating an Account Definition 21
Master Data for an Account Definition 21
Setting Up Manage Levels 24
Master Data for a Manage Level 25
Creating a Formatting Rule for IT Operating Data 26
Determining IT Operating Data 27
Modifying IT Operating Data 29
Assigning Account Definitions to Employees 30
Assigning Account Definitions to Departments, Cost Centers and Locations 31
Assigning Account Definitions to Business Roles 31
Assigning Account Definitions to all Employees 32
Assigning Account Definitions Directly to Employees 33
Assigning Account Definitions to System Roles 33
Adding Account Definitions in the IT Shop 34
Assigning an Account Definition to a Custom Target System 35
Deleting an Account Definition 36
Password Policies 37
Predefined Password Policies 38
Editing Password Policies 39

General Master Data for a Password Policy 39
Policy Settings 40
Character Sets for Passwords 40
Custom Scripts for Password Requirements 41
Script for Checking a Password 41
Script for Generating a Password 43
Restricted Passwords 44
Testing a Password 44
Testing Generating a Password 44
Assigning a Password Policy 45
Initial Password for New User Accounts 46
Email Notifications about Login Data 48
Target System Managers 49
Target system types 52
Displaying Customized Schema Extension for Custom Target Systems 53

Setting up a Custom Target System 55
General Master Data for a Custom Target System 56
Customizing Data Synchronization for a Custom Target System 58
Specifying Categories for Inheriting Groups 58
Alternative Column Names 59

Container Structures in a Custom Target System 60
Master Data for a Container 60

User Accounts in a Custom Target System 62
Linking User Accounts to Employees 62
Supported User Account Types 63
Entering Master Data for User Accounts 66
User Account Master Data 67
Additional Tasks for Managing User Accounts 70
Overview of User Accounts 70
Changing the Manage Level of a User Account 70
Assigning Groups directly to User Accounts 71
Assigning Extended Properties 71
Assigning Permissions Controls 72
Automatic Assignment of Employees to User Accounts 72

Editing Search Criteria for Automatic Employee Assignment 75
Disabling User Accounts 77
Deleting and Restoring User Accounts 78

Groups in a Custom Target System 80
Group Master Data 80
Assigning Group to User Accounts 81
Assigning Groups to Departments, Cost Centers and Locations 82
Assigning Groups to Business Roles 83
Assigning User Accounts to a Group 84
Add Groups to System Roles 84
Adding Groups to the IT Shop 85
Additional Tasks for Managing Groups 86
Overview of Groups 86
Adding Groups to Groups 86
Effectiveness of Group Memberships 87
Group Inheritance Based on Categories 89
Assigning Extended Properties 91
Assigning Permissions Controls 91

Entering Permissions Controls 93
Permissions Control Master Data 93
Additional Tasks for Permissions Controls 94
Permissions Control Overview 94
Assigning Permissions Controls to User Accounts 94
Assigning Permissions Controls to Groups 95

Reports about Custom Target Systems 96
Overview of all Assignments 97

Appendix: Configuration Parameters for Managing Custom Target Systems 99

About us 101
Contacting us 101
Technical support resources 101

Index 102

Managing Custom Target Systems

You can also map your own implementations, such as telephone systems, in One Identity Manager along side native target systems. To manage these target systems with One Identity Manager, create container structures, user accounts and groups.

Define a custom process to swap data between the target system and the One Identity Manager database.

- 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.
- Alternatively, you can configure data imports with the program "Data Import" or set up synchronization using the CSV connector in the Synchronization Editor. This requires a large amount of customizing. .

The One Identity Manager components for managing custom target systems are available if the configuration parameter "TargetSystem\UNS" is set.

- Check whether the configuration parameter is set in the Designer. Otherwise, set the configuration parameter and compile the database.
- Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.

One Identity Manager Users for Managing Custom Target Systems

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

Table 1: User

User	Task
Target system admin-	Target system administrators must be assigned to the

User	Task
istrators	application role **Target system | Administrators**. Users with this application role: • Administrate application roles for individual target systems types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles are conflicting for target system managers • Authorize other employee 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 application role **Target systems | Custom target systems** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare groupssystem entitlements for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines 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.
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, as required. • Enable or disable additional configuration parameters in

User	Task
	the Designer, as required. • Create custom processes in the Designer, as required. • Create and configures schedules, as required. • Create and configure password policies, as required.
Administrators for the IT Shop	Administrators must be assigned to the application role **Request & Fulfillment | IT Shop | Administrators**. Users with this application role: • Assign groups to IT Shop structures.
Administrators for organizations	Administrators must be assigned to the application role **Identity Management | Organizations | Administrators**. Users with this application role: • Assign groups to departments, cost centers and locations.
Business roles administrators	Administrators must be assigned to the application role **Identity Management | Business roles | Administrators**. Users with this application role: • Assign groups to business roles.

2

Setting up Script Controlled 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:

- Create provisioning scripts

  Data provisioning from One Identity Manager into a custom target system is done by scripts. These must be created for each target system. For more information, see Creating the Script for Data Provisioning in a Custom Target System on page 10.

- Providing a server for provisioning

  The One Identity Manager Service must be installed, configured and started on the server. The server must be declared in One Identity Manager and entered as the synchronization server in the target system. For more information, see Setting up a Server for Data Provisioning in a Custom Target System on page 11.

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

  Select the synchronization method "Synchronization by script". For more information, see Setting up a Custom Target System on page 55.

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

Creating the Script for Data Provisioning in a Custom Target System

In the 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 script `TSB_Uns_Generic_Templates` 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 into the custom target system "Telephone system"

`CCC_UNSAccountB_Telephonesystem_Insert`

> IMPORTANT: If your target system contains a hyphen ("-") in it's name, you must remove it from the script function in the part `<Ident_UNSRoot>`. 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.
UNSAccountBHasUNSItemB	Permissions control assignments to user accounts.
UNSAccountBInUNSGroupB	Group assignments to user accounts.
UNSContainerB	Container structure mapping.
UNSGroupB	Group mapping.
UNSGroupBHasUnsItemB	Permissions control assignments to groups.
UNSGroupBInUNSGroupB	Group assignments to groups.
UNSItemB	Mapping of additional permissions controls.
UNSRootB	Basis for mapping custom target systems.

Setting up a Server for Data Provisioning in a Custom Target System

You can define a server for each custom target system, which executes all the One Identity Manager Service actions required for provisioning target system objects.

To set up a server

1. Provide a server installed with the One Identity Manager Service.
2. Create an entry for the Job server in the Manager.
    a. Select the category **Custom target systems | Basic configuration data | Servers**.
    b. Click in the result list toolbar.
    c. Edit the Job server's master data.
    d. Save the changes.
3. Enter the server as the synchronization server in the custom target system.

Detailed information about this topic

- Master Data for a Job Server on page 11
- Customizing Data Synchronization for a Custom Target System on page 58
- For more detailed information about installing and configuring the One Identity Manager Service, see the One Identity Manager Installation Guide.

Master Data for a Job Server

NOTE: All editing options are available to you in the Designer, in the category **Base Data | Installation | Job server**.

Table 3: Job Server Properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: `<Name of servers>.<Fully qualified domain name>`
Target System	Computer account target system.

Property	Meaning
Language culture	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 properties **Server is cluster** and **Server belongs to cluster** 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. Only the methods "Robocopy" and "Rsync" are currently supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication then takes place between servers with a Windows operating system using "Robocopy" and between servers with the Linux operating system using "rsync". 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 executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when One Identity Manager Service is 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. Each One Identity Manager

Property	Meaning
	Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. 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. Permitted values are "Win32", "Windows", "Linux" and "Unix". If the input is empty, "Win32" is assumed.
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 procedure `QBM_PJobQueueLoad` 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 program "Job Queue Info".
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 running	Specifies whether a software update is currently being executed.
Server Function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related Topics

- Specifying Server Functions on page 13

Specifying Server Functions

NOTE: All editing options are available to you in the Designer, in the category **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 controller are considered to be member servers.
Printer server	Server which 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 executes automatic software updating of all other servers. The server requires a direct connection to the database server that the One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.
SQL processing server	This server can process SQL tasks. 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.
Native database connector	The server can connect to an ADO.Net database.
One Identity Manager database connector	Server on which the One Identity Manager connector is installed. This server executes synchronization with the target system One Identity Manager.
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 for running synchronization with an SMB-based target system.

Server Function	Remark
Server	
SMTP host	Server from which the One Identity Manager Service sends email notifications. Prerequisite for sending mails using the 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.

Objects marked as outstanding:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronization.
- Must be post-processed separately in One Identity Manager.

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.

  For more information, see Configuring Target System Synchronization on page 16.

Related Topics

- Target system types on page 52
- Post-Processing Outstanding Objects on page 16

Configuring 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 tables for which outstanding objects can be published in the target system during post-processing.

To add tables to the target system synchronization.

1. Select the category **Custom target systems | Basic configuration data | Target system types**.
2. Select the target system type of the custom target system in the result list.
3. Select **Assign synchronization tables** in the task view.
4. Assign tables whose outstanding objects you want to handle in **Add assignments**.
5. Save the changes.
6. Select **Configure tables for publishing**.
7. Select tables whose outstanding objects can be published in the target system and set the option **Publishable**.
8. Save the changes.

To publish outstanding objects

- Create a process for each table with outstanding objects you want to publish. The process is triggered by the event "HandleOutstanding" and provisions the objects. Use the process function "AdHocProjection" of the process component "ProjectorComponent". For more detailed information about defining processes, see One Identity Manager Configuration Guide.

NOTE: You must set up matching processes in One Identity Manager to publish outstanding objects that are being post-processed. For more information, see Setting up Script Controlled Data Provisioning in a Custom Target System on page 9.

If you use the CSV connector for provisioning, ensure that the CSV connector has write access to the CSV files. That means, the option **Connection is read only** must no be set for the target system connection. For more information, see theOne Identity Manager Target System Synchronization Reference Guide.

Post-Processing Outstanding Objects

To post-process outstanding objects

1. Select the category **Custom target systems | Basic configuration data | Target system synchronization: <Target system>**.

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

2. Select the table whose outstanding objects you want to edit in the navigation view.

   All objects marked as outstanding are shown on the form.

   TIP:

   To display object properties of an outstanding object

   a. Select the object on the target system synchronization form.

   b. Open the context menu and click **Show object**.

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

Table 5: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted in the One Identity Manager. Deferred deletion is not taken into account. The "outstanding" label is removed from the object. Indirect memberships cannot be deleted.
	Publish	The object is added in the target system. The "outstanding" label is removed from the object. The method triggers the event "HandleOutstanding". 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 from the object.

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

NOTE: By default, the selected objects are processed in parallel, which speeds up execution of 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

- Deactivate in the form toolbar.

Related Topics

- Configuring Target System Synchronization on page 16

3

Base Data for Custom Target Systems

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

- Configuration parameter

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

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

  For more information, see Appendix: Configuration Parameters for Managing Custom Target Systems on page 99.

- Account definitions

  One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not have a user account in the target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling.

  For more information, see Setting Up Account Definitions on page 20.

- Password policies

  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 user or customize if required. You can also define your own password policies.

  For more information, see Password Policies on page 37.

- Initial Password for New User Accounts

  You have the different options for issuing an initial password for user accounts. The central password of the assigned employee can be aligned with the user account password, a predefined, fixed password can be used or a randomly generated initial password can be issued.

  For more information, see Initial Password for New User Accounts on page 46.

- Email notifications about login data

  When a new user account is created, the login data are send 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 48.

- 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 Setting up a Server for Data Provisioning in a Custom Target System on page 11.

- Target system managers

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

  Define other application roles, if you want to limit target system managers' access permissions to individual target system managers. The application roles must be added under the default application role.

  For more information, see Target System Managers on page 49.

- Target system types

  Target system types for groups custom target systems. You can assign user accounts to groups belonging to different target systems within a target system type. For more information, see Target system types on page 52.

- Custom schema extensions to base tables

  You can display custom columns in tables `UNSAccountB`, `UNSContainerB`, `UNSGroupB`, `UNSItemB` and `UNSRootB` in the Manager. To do this, modify the custom column's column definition. For more information, see Displaying Customized Schema Extension for Custom Target Systems on page 53.

Setting Up Account Definitions

One Identity Manager has account definitions for automatically allocating user accounts to employees during working hours. You can create account definitions for every target system. If an employee does not have a user account in the target system, a new user

account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling.

The data for the user accounts in the respective target system comes from the basic employee data. 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 (template processing). 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.

For more details about the basics, see the One Identity Manager Target System Base Module Administration Guide.

The following steps are required to implement an account definition:

- Creating an Account Definition
- Setting Up Manage Levels
- Creating a Formatting Rule for IT Operating Data
- Determining IT Operating Data
- Assigning Account Definitions to Employees
- Assigning an Account Definition to a Custom Target System

Creating an Account Definition

To create a new account definition

1. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Enter the account definition's master data.
4. Save the changes.

Detailed information about this topic

- Master Data for an Account Definition on page 21

Master Data for an Account Definition

Enter the following data for an account definition:

Table 6: Master Data for an Account Definition

Property	Description
Account definition	Account definition name.
User account table	Table in the One Identity Manager schema which maps user accounts.
Target System	Target system to which the account definition applies.
Required account definition	Required account definitions. Define the dependencies between account definitions. When this account definition is requested or assigned, the required account definition is automatically requested or assigned with it.
Description	Spare text box 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 account definition assignments to employees. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.
Service item	Service item through which you can request the account definition 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 ordered by an employee over the Web Portal and distributed using a defined approval process. The account definition can still be directly assigned 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 ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added.

Property	Description
	IMPORTANT: Only set this option 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. Disable this option to remove automatic assignment of the account definition to all 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 disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: 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 disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: 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 stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
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 stays the same. Option not set: 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.

Setting Up Manage Levels

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.

The One Identity Manager supplies a default configuration for manage levels:

- Unmanaged

  User accounts with a manage level of "Unmanaged" become linked to an employee but do not inherit any other 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 a manage level of "Full managed" inherit specific properties from the assigned employee.

NOTE: The manage levels "Full managed" and "Unmanaged" are evaluated in the 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.

- 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 assign manage levels to an account definition

1. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign manage level** in the task view.

4. Assign manage levels in **Add assignments**.

   - OR -

   Remove assignments to manage levels in **Remove assignments**.
5. Save the changes.

IMPORTANT: The manage level "Unmanaged" is assigned automatically when an account definition is assigned and cannot be removed.

To edit a manage level

1. Select the category **Custom Target Systems | Basic configuration data | Account definitions | Manage level**.
2. Select the manage level in the result list. Select **Change master data**.

   - OR -

   Click in the result list toolbar.
3. Edit the manage level's master data.
4. Save the changes.

Related Topics

- Master Data for a Manage Level on page 25

Master Data for a Manage Level

Enter the following data for a manage level.

Table 7: Master Data for a Manage Level

Property	Description
Manage level	Name of the manage level.
Description	Spare text box 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 always: Data is always updated Only initially: Data is only initially determined.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.

Property	Description
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled 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 locked user accounts retain their group memberships.

Creating a Formatting Rule 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 automatic creating and modifying of user accounts for an employee in the target system.

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

To create a mapping rule for IT operating data

1. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Edit IT operating data mapping** in the task view and enter the following

data.

Table 8: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set.
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: Only use the primary business role if the Business Roles Module is installed. • Empty If you select a role, you must specify a default value and set the option **Always use default value**.
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 user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. Use the mail template "Employee - new user account with default properties created". To change the mail template, modify the configuration parameter "TargetSystem\UNS\Accounts\MailTemplateDefaultValues".

4. Save the changes.

Related Topics

- Determining IT Operating Data on page 27

Determining IT Operating Data

In order for an employee to create user accounts with the manage level "Full managed", the necessary IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, cost centers, and business roles. An employee is assigned to one primary

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

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

Example:

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

Create an account definition A for the default user account of the domain A and an account definition B for the administrative user account of domain A. Specify the property "Department" in the IT operating data formatting rule for the account definitions A and B in order to determine the valid IT operating data.

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

To specify IT operating data

1. Select the role in the category **Organizations** or **Business roles**.
2. Select **Edit IT operating data** in the task view and enter the following data.

Table 9: IT Operating Data

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

Property	Description
Value	Concrete value which is assigned to the user account property.

3. Save the changes.

Related Topics

- Creating a Formatting Rule for IT Operating Data on page 26

Modifying IT Operating Data

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

Prerequisites

- The IT operating data of a department, cost center, business role or a location was changed.

  - OR -

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

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

To execute the template

1. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Execute templates** in the task view

   This displays a list of all user account, which are created through the selected account definition and whose properties are changed by modifying the IT operating data.

Old value	Current value of the object property.
New	Value applied to the object property after modifying the IT operating

value	data.
Selection	Specifies whether the modification is applied to the user account.

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

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

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. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

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. You have to alter the user account manage level afterwards in this case.

Prerequisites for indirect assignment of account definitions to employees

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

For detailed 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 31
- Assigning Account Definitions to Business Roles on page 31
- Assigning Account Definitions to all Employees on page 32

- Assigning Account Definitions Directly to Employees on page 33
- Assigning an Account Definition to a Custom Target System on page 35

Assigning Account Definitions to Departments, Cost Centers and Locations

To add account definitions to hierarchical roles

1. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

   Remove the organizations from **Remove assignments**.
5. Save the changes.

Related Topics

- Assigning Account Definitions to Business Roles on page 31
- Assigning Account Definitions to all Employees on page 32
- Assigning Account Definitions Directly to Employees on page 33

Assigning Account Definitions to Business Roles

Installed Modules: Business Roles Module

To add account definitions to hierarchical roles

1. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

Remove business roles in **Remove assignments**.

5. Save the changes.

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 31
- Assigning Account Definitions to all Employees on page 32
- Assigning Account Definitions Directly to Employees on page 33

Assigning Account Definitions to all Employees

To assign an account definition to all employees

1. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Automatic assignment to employees** on the **General** tab.

   IMPORTANT: Only set this option 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.

5. Save the changes.

The account definition is assigned to every employee that is not marked as external. New employees automatically obtain this account definition as soon as they are added. The assignment is calculated by the DBQueue Processor.

NOTE: Disable the option **Automatic assignment to employees** to remove automatic assignment of the account definition to all employees. 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 31
- Assigning Account Definitions to Business Roles on page 31
- Assigning Account Definitions Directly to Employees on page 33

Assigning Account Definitions Directly to Employees

To assign an account definition directly to employees

1. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign to employees** in the task view.
4. Assign employees in **Add assignments**.

   - OR -

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 31
- Assigning Account Definitions to Business Roles on page 31
- Assigning Account Definitions to all Employees on page 32

Assigning Account Definitions to System Roles

Installed Modules: System Roles Module

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

To add account definitions to a system role

1. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove assignments to system roles in **Remove assignments**.
5. Save the changes.

Adding Account Definitions in the IT Shop

A 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.
- If the account definition is only assigned to employees using IT Shop assignments, you must also set the option **Only for use in IT Shop**. 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

1. Select the category **Custom Target Systems | Basic configuration data | Account definitions | Account definitions** (non role-based login).

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the account definition to the IT Shop shelf in **Add assignments**
5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. Select the category **Custom Target Systems | Basic configuration data | Account definitions | Account definitions** (non role-based login).

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the account definition from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove an account definition from all IT Shop shelves

1. Select the category **Custom Target Systems | Basic configuration data | Account definitions | Account definitions** (non role-based login).

   - OR -

   Select the category **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.

3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

For more detailed information about request from company resources through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Related Topics

- Master Data for an Account Definition on page 21
- Assigning Account Definitions to Departments, Cost Centers and Locations on page 31
- Assigning Account Definitions to Business Roles on page 31
- Assigning Account Definitions Directly to Employees on page 33
- Assigning Account Definitions to System Roles on page 33

Assigning an Account Definition to a Custom Target System

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

- 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 (state "Linked") 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. Select the target system in the category **Custom target systems**.
2. Select **Change master data** in the task view.
3. Select the account definition for user accounts from **Account definition (initial)**.
4. Save the changes.

You must customize automatic assignment of employees to user accounts for custom target systems.

Detailed information about this topic

- Automatic Assignment of Employees to User Accounts on page 72

Deleting an Account Definition

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

NOTE: If an account definition is deleted, the user accounts arising from this account definition are deleted.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
    a. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Change master data** in the task view.
    d. Disable the option **Automatic assignment** to employees on the **General** tab.
    e. Save the changes.
2. Remove direct assignments of the account definition to employees.
    a. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign to employees** in the task view.
    d. Remove employees from **Remove assignments**.
    e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers and locations.
    a. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign organizations**.
    d. Remove the account definition's assignments to departments, cost centers and locations in **Remove assignments**.
    e. Save the changes.
4. Remove the account definition's assignments to business roles.
    a. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
    b. Select an account definition in the result list.
    c. Select **Assign business roles** in the task view.

    Remove business roles from **Remove assignments**.

d. 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, see the One Identity Manager IT Shop Administration Guide.
6. Remove the account definition assignment as required account definition for another account definition. As long as the account definition is required for another account definition, it cannot be deleted. Check all the account definitions.
   a. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
   b. Select an account definition in the result list.
   c. Select **Change master data** in the task view.
   d. Remove the account definition from the **Required account definition** menu.
   e. Save the changes.
7. Remove the account definition's assignments to target systems.
   a. Select the target system in the category **Custom target systems**.
   b. Select **Change master data** in the task view.
   c. Remove the assigned account definitions on the **General tab**.
   d. Save the changes.
8. Delete the account definition.
   a. Select the category **Custom target systems | Basic configuration data | Account definitions | Account definitions**.
   b. Select an account definition in the result list.
   c. Click , to delete the account definition.

Password Policies

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 user or customize if required. You can also define your own password policies.

Detailed information about this topic

- Predefined Password Policies on page 38
- Editing Password Policies on page 39
- Custom Scripts for Password Requirements on page 41

- Restricted Passwords on page 44
- Testing a Password on page 44
- Testing Generating a Password on page 44
- Assigning a Password Policy on page 45

Predefined Password Policies

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

Password for logging into One Identity Manager

The password policy "One Identity Manager password policy" is used for logging into One Identity Manager. This password policy defined the settings for the system user passwords (`DialogUser.Password` and `Person.DialogUserPassword`) as well as the access code for a one off log in on the Web Portal (`Person.Passcode`).

The password policy "One Identity Manager password policy" is also labeled as the default and is used when no other password policy is found.

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 password policy "Employee central password policy" defines the settings for the central password (`Person.CentralPassword`).

IMPORTANT: Ensure that the password policy "Employee central password policy" does not violate the target system specific password requirements.

Password policies for target systems

IMPORTANT: If you are not working with target system specific password policies, the default policy applies. In this case, ensure that the password policy "One Identity Manager password policy" does not violate the target system 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.

Editing Password Policies

To edit a password policy

1. Select the category **Custom target systems | Basic configuration data | Password policies** in the Manager.
2. Select the password policy in the result list and select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Edit the password policy's master data.
4. Save the changes.

Detailed information about this topic

- General Master Data for a Password Policy on page 39
- Policy Settings on page 40
- Character Sets for Passwords on page 40
- Custom Scripts for Password Requirements on page 41

General Master Data for a Password Policy

Enter the following master data for a password policy.

Table 10: Master Data for a Password Policy

Property	Meaning
Display name	Password policy name. Translate the given text using the button.
Description	Spare text box for additional explanation. Translate the given text using the button.
Error Message	Custom error message outputted if the policy is not fulfilled. 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. NOTE: The password policy "One Identity Manager password policy" is marked as the default policy. This password policy is applied if no other password policies can be found.

Policy Settings

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

Table 11: Policy Settings

Property	Meaning
Initial password	Initial password for new user accounts. If no password is given when the user account is added or a random password is generated, the initial password is used.
Password confirmation	Reconfirm password.
Min. Length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have.
Max. errors	Maximum number of errors. Set the number of invalid passwords. If the user has reached this number the user account is blocked.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
Password history	Enter the number of passwords to be saved. If the value '5' is entered, for example, the last 5 passwords of the user are saved.
Min. password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The password strength is not tested if the value is '0'. The values '1', '2', '3' and '4' gauge the required complexity of the password. The value '1' demands the least complex password. The value '4' demands the highest complexity.
Name properties denied	Specifies whether name properties are permitted in the password.

Character Sets for Passwords

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

Table 12: Character Classes for Passwords

Property	Meaning
Min. letters	Specifies the minimum number of alphabetical characters

Property	Meaning
	the password must contain.
Min. number lower case	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 characters.
Denied special characters	List of characters, which are not permitted.
Max. identical characters in total	Maximum number of identical characters that can be present in the password in total.
Max. identical characters in succession	Maximum number of identical character that can be repeated after each other.

Custom Scripts for Password Requirements

You can implement custom scripts for testing and generating password 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

- Script for Checking a Password on page 41
- Script for Generating a Password on page 43

Script for Checking a Password

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

Syntax for 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 test

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

Example for a script for testing a password

A password cannot have '?' or '!' at the beginning. 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. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select the category **Custom target systems | Basic configuration data | Password policies** in the Manager.
    b. Select the password policy in the result list.
    c. Select **Change master data** in the task view.
    d. Enter the name of the script to test the password in **Check script** on the **Scripts** tab.
    e. Save the changes.

Related Topics

- Script for Generating a Password on page 43

Script for Generating a Password

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 property `Entity` of the `PasswordPolicy` class.

Example for a script to generate a password

The script replaces the invalid characters '?' and '!' in random passwords.

```
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. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select the category **Custom target systems | Basic configuration data | Password policies** in the Manager.
    b. Select the password policy in the result list.
    c. Select **Change master data** in the task view.
    d. Enter the name of the script to generate a password in **Generation script** on the **Scripts** tab.
    e. Save the changes.

Related Topics

- Script for Checking a Password on page 41

Restricted Passwords

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. Select the category **Base Data | Security Settings | Restricted passwords** in the Designer.
2. Create a new entry with the menu item **Object | New** an enter the term to excluded to the list.
3. Save the changes.

Testing a Password

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

To test whether a password conforms to the password policy

1. Select the category **Custom target systems | Basic configuration data | Password policies** in the Manager.
2. Select the password policy in the result list.
3. Select **Change master data** in the task view.
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 Generating a Password

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. Select the category **Custom target systems | Basic configuration data | Password policies** in the Manager.
2. Select the password policy in the result list.
3. Select **Change master data** in the task view.
4. Select the **Test** tab.
5. Click **Generate**.

   This generates and displays a password.

Assigning a Password Policy

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.

IMPORTANT: If you are not working with target system specific password policies, the default policy applies. In this case, ensure that the password policy "One Identity Manager password policy" does not violate the target system requirements.

To reassign a password policy

1. Select the category **Custom target systems | Basic configuration data | Password policies** in the Manager.
2. Select the password policy in the result list.
3. Select **Assign objects** in the task view.

4. Click **Add** in the **Assignments** section and enter the following data.

Table 13: Assigning a Password Policy

Property	Description
Apply to	Application scope of the password policy. ***To specify an application scope*** a. Click → next to the text box. b. Select the table which contains the password column under **Table**. c. Select the specific target system under **Apply to**. d. Click **OK**.
Password column	The password column's identifier.
Password policy	The identifier of the password policy to be used.

5. Save the changes.

To change a password policy's assignment

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

Initial Password for New User Accounts

Table 14: Configuration Parameters for Formatting Initial Passwords for User Accounts

Configuration parameter	Meaning
QER\Person\UseCentralPassword	This configuration parameter specifies whether the employee's central password is used in the user accounts. The employee's central password is automatically mapped to the employee's user account in all permitted target systems. This excludes privileged user accounts, which are not

Configuration parameter	Meaning
	updated.
QER\Person\UseCentralPassword\PermanentStore	This configuration parameter controls the storage period for central passwords. If the parameter is set, the employee's central password is permanently stored. If the parameter is not set, the central password is only used for publishing to existing target system specific user accounts and is subsequently deleted from the One Identity Manager database.
TargetSystem\UNS\Accounts\InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. It must contain at least those character sets set in the configuration subparameters.

You have the following possible options for issuing an initial password for a new user account.

- User the employee's central password. The employee's central password is mapped to the user account password.
  - Set the configuration parameter "QER\Person\UseCentralPassword" in the Designer.

    If the configuration parameter "QER\Person\UseCentralPassword" is set, the employee's central password is automatically mapped to an employee's user account in each of the target systems. This excludes privileged user accounts, which are not updated.
  - Use the configuration parameter "QER\Person\UseCentralPassword\PermanentStore" in the Designer to specify whether an employee's central password is permanently saved in the One Identity Manager database or only until the password has been published in the target system.

  The password policy "Employee central password policy" is used to format the central password.

  IMPORTANT: Ensure that the password policy "Employee central password policy" does not violate the target system specific password requirements.
- Create user accounts manually and enter a password in their master data.
- Specify an initial password to be used when user accounts are created automatically.
  - Apply the target system specific password policies and enter an initial password in the password policies.
- Assign a randomly generated initial password to enter when you create user accounts.

- Set the configuration parameter "TargetSystem\UNS\Accounts\InitialRandomPassword" in the Designer.
- 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 on page 37
- Email Notifications about Login Data on page 48

Email Notifications about Login Data

Table 15: Configuration Parameters for Notifications about Login Data

Configuration parameter	Meaning
TargetSystem\UNS\Accounts\InitialRandomPassword\SendTo	This configuration parameter specifies to which employee the email with the random generated password should be sent (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	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account). Use the mail template "Employee - new account created".
TargetSystem\\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password). Use the mail template "Employee - initial password for new user account".
TargetSystem\UNS\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.

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, which 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.

To use email notifications about login data

1. Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the One Identity Manager Configuration Guide.
2. Enable the configuration parameter "Common\MailNotification\DefaultSender" in the Designer and enter the email address for sending the notification.
3. Ensure that all employees have a default email address. Notifications are sent to this address. For more detailed information, see the One Identity Manager Identity Management Base Module Administration Guide.
4. Ensure that a language culture can be determined for all employees. Only then can they receive email notifications in their own language. For more detailed 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. Set the configuration parameter "TargetSystem\UNS\Accounts\InitialRandomPassword" in the Designer.
2. Set the configuration parameter "TargetSystem\UNS\Accounts\InitialRandomPassword\SendTo" in the Designer and enter the message recipient as the value.
3. Set the configuration parameter "TargetSystem\UNS\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName" in the Designer.

   By default, the message sent uses the mail template "Employee - new account created". The message contains the name of the user account.
4. Set the confiugration parameter "TargetSystem\UNS\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword" in the Designer.

   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: Change the value of the configuration parameter in order to use custom mail templates for these mails.

Target System Managers

For more detailed information about implementing and editing application roles, see the One Identity Manager Application Roles Administration Guide.

Implementing Application Roles for Target System Managers

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

   The default application role target system managers are entitled to edit all target systems in One Identity Manager.
3. Target system managers can authorize more employees as target system managers, within their scope of responsibilities and create other child application roles and assign individual target systems.

Table 16: Default Application Roles for Target System Managers

User	Task
Target System Managers	Target system managers must be assigned to the application role **Target systems | Custom target systems** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare groupssystem entitlements for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines 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 One Identity Manager administrator (application role **Base role | Administrators**)
2. Select the category **One Identity Manager Administration | Target systems | Administrators**.
3. Select **Assign employees** in the task view.
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 yourself into the Manager as target system administrator (application role **Target systems | Administrator**).
2. Select the category **One Identity Manager Administration | Target systems | Custom target systems**.
3. Select **Assign employees** in the task view.
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. Login to the Manager as target system manager.
2. Select the application role in the category **Custom Target Systems | Basic configuration data | Target system managers** .
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

To define target system managers for individual target systems.

1. Login to the Manager as target system manager.
2. Select the category **Custom target systems | Basic configuration data | Target systems**.
3. Select the target system in the result list.
4. Select **Change master data** in the task view.
5. Select the application role on the **General** tab in the **Target system manager** menu.

   - OR -

   Click next to the **Target system manager** menu to create a new application role.
   - Enter the application role name and assign the parent application role **Target systems | Custom target systems**.
   - Click **OK** to add the new application role.
6. Save the changes.
7. Assign the application role to employees, who are authorized to edit the target system in One Identity Manager.

Related Topics

- One Identity Manager Users for Managing Custom Target Systems on page 6
- General Master Data for a Custom Target System on page 56

Target system types

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. In addition, tables containing outstanding objects are maintained on target system types. For more information, see Post-Processing Outstanding Objects on page 15.

To assign user accounts to system entitlements with a target system type

- Define a target system type.
- Assign target systems to the target system type.

To edit target system types

1. Select the category **Custom target systems | Basic configuration data | Target system types**.
2. Select the target system type in the result list.

   - OR -

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

   Table 17: Master Data for a Target System Type

Property	Description
Target system type	Target system type description.
Description	Spare text box for additional explanation.
Display Name	Name of the target system type as displayed in One Identity Manager tools.
Cross boundary inheritance	Specifies whether user accounts can be assigned to groups if they belong to different custom target systems. NOTE: If this option is not set, the target system type is used to group 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.

4. Save the changes.

To assign a custom target system to a target system type

1. Select the category **Custom target systems | Basic configuration data | Target systems**.
2. Select a target system in the result list.
3. Select **Change master data** in the task view.
4. Select **Target system type** from the target system type to which you want to assign the target system.
5. Save the changes.

Displaying Customized Schema Extension for Custom Target Systems

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

See the One Identity Manager Configuration Guide for detailed information about extending tables with custom columns using the program "Schema Extension" and about customizing column definitions with the program "Designer".

To display custom columns for the tables `UNSAccountB`, `UNSContainerB`, `UNSGroupB`, `UNSItemB` and `UNSRootB` on forms in the Manager

- Specify the order for displaying input fields in the Designer in the property **Sort order** (`DialogColumn.SortOrder`). Columns with a sort order of less that one are not displayed.
- Modify the property **Group** (`DialogColumn.ColumnGroup`) in the Designer in the custom column's column definition. The group determines, which tab the column will appear on.
    - If you do not specify a group, 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

The table UNSAccountB is extended by 5 columns. The columns should be displayed as follows for target system type A, target system type B and target system type C.

- Column 1 on the "Custom" tab for all target system types.
- Column 2 on the tab "Group A" for all target system types.
- Column 3 on the tab "Target system type B" for the target system type B. Columns are not displayed for target system type A and target system type C.
- Column 4 on the tab "Target system type B" for target system type B and on the tab "Target system type C" for target system type C. The column is not displayed for target system type A.
- Column 5 on the tab "Group A" for target system type B and target system type C. The column is not displayed for target system type A.

Table 18: 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

Setting up a Custom Target System

Table 19: Configuration Parameters for Target System Identification

Configuration parameter	Meaning
TargetSystem\UNS\CreateNewRoot	The configuration parameter specifies whether new target systems can be added. If this parameter is set, custom target systems can be added.

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

- Select the configuration parameter "TargetSystem\UNS\CreateNewRoot" in the Designer.

To edit target system identifiers

1. Select the category **Custom target systems | Basic configuration data | Target systems**.
2. Select a target system in the result list. Select **Change master data** in the task view.

   - OR -

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

TIP: You can also edit target system properties in the category **Custom target systems | <target system>**.

Detailed information about this topic

- General Master Data for a Custom Target System on page 56
- Customizing Data Synchronization for a Custom Target System on page 58
- Specifying Categories for Inheriting Groups on page 58
- Alternative Column Names on page 59

General Master Data for a Custom Target System

Enter the following data for a custom target system.

Table 20: Custom Target System Master 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.master system name`
	Example
	`DHW2k01.Testlab.com`

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. These account definitions are used if automatic assignment of employees to user account is used for this domain resulting in administered user accounts (state "Linked configured"). The account definition's default manage level is applied. User accounts are only linked to the employee (state "Linked") if no account definition is given. This is the case on initial synchronization, for

Property	Description
	example.
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	NOTE: You can only specify the synchronization type when adding a new custom target system. No changes can be made after saving. Type of synchronization through which the data is synchronized between the target system and One Identity Manager. **Table 21: Permitted Values** **Value** / **Synchronization by** / **Provisioned by** Synchronization by script / none / One Identity Manager script components No synchronization / none / none If you select "Synchronize by script" you can define custom 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.
Description	Spare text box for additional explanation.
Group memberships as MVP	Specifies whether group memberships can be grouped together as a list on an multi-valued property column of this target system's user accounts (relevant for data import).

Related Topics

- Target system types on page 52
- Automatic Assignment of Employees to User Accounts on page 72
- Target System Managers on page 49

Customizing Data Synchronization for a Custom Target System

At this point, 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 22: Data Synchronization Master 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. This option is only relevant if the connection target system is synchronized by script.

Related Topics

- Setting up a Server for Data Provisioning in a Custom Target System on page 11

Specifying Categories for Inheriting Groups

In One Identity Manager, groups can be selectively inherited by user accounts. For this, groups and user accounts are divided into categories. The categories can be freely selected and are specified by a template. Each category is given a specific position within the template. The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. Enter your categories for the target system dependent groups, administrative roles, subscriptions and disabled service plans in the . Each table contains the category items "Position1" to "Position31".

To define a category

1. Select the category **Custom target systems | Basic configuration data | Target systems**.
2. Select a target system in the result list.
3. Select **Change master data** in the task view.
4. Switch to the **Mapping rule category** tab.

5. Expand the respective base node of the user account or group table.
6. Click to enable category.
7. Enter a name for the user account and group categories in the current language.
8. Save the changes.

Detailed information about this topic

- Group Inheritance Based on Categories on page 89

Alternative Column Names

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

To specify alternative column names

1. Select the category **Custom target systems | Basic configuration data | Target systems**.
2. Select a target system in the result list. Select **Change master data** in the task view.
3. Select the tab **Alternative column names**.
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 a Custom Target System

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

To edit container master data

1. Select the category **Custom target systems | <target system> | Container structure**.
2. Select the container in the result list and run **Change master data** in the task view.

   - OR -

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

Detailed information about this topic

- Master Data for a Container on page 60

Master Data for a Container

Enter the following master data for a container.

Table 23: Master Data for a Container

Property	Description
Name	Container name.
Canonical name	Container's canonical name. The canonical name is generated automatically and should not be changed.

Property	Description
Distinguished name	Container's distinguished name. The distinguished name is determined using a template and must not be changed.
Parent container	Parent container for mapping a hierarchical container structure. The distinguished name is automatically updated using templates.
Description	Spare text box for additional explanation.

6

User Accounts in a Custom Target System

User accounts represent a target system's authentication objects. A user receives access to target system resources through group memberships and access permissions.

Related Topics

- For more information, see Linking User Accounts to Employees on page 62.
- Supported User Account Types on page 63
- Entering Master Data for User Accounts on page 66

Linking User Accounts to Employees

The central component of the One Identity Manager is to map employees and their master data with permissions through which they have control over different target systems. For this purpose, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This gives an overview of the permissions for each employees in all of the connected target systems. One Identity Manager provides the possibility to manage 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, the One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following method for linking employees and their user accounts.

- Employees and user accounts can be entered manually and assigned to each other.
- Employees can automatically obtain their account definitions using user account resources. If an employee does not 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 mechanism followed by process handling.

When you manage account definitions through user accounts, you can specify the way user accounts behave when employees are enabled or deleted.

NOTE: If employees obtain their user accounts through account definitions, they have to have a central user account and obtain their company IT data through assignment to a primary department, primary location or a primary cost center.

Related Topics

- Setting Up Account Definitions on page 20
- Entering Master Data for User Accounts on page 66
- Automatic Assignment of Employees to User Accounts on page 72
- For more detailed information about handling and administration of employees and user accounts, see the One Identity Manager Target System Base Module Administration Guide.

Supported User Account Types

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

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

- Identity (column `IdentityType`)

  The identity describes the type of user account.

Table 24: Identities of User Accounts

Identity	Description	Value of the column "IdentityType"
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for various roles within the organization, f. ex. In sub-agreements with other functional areas.	Organizational
Personalized admin identity	User account with administration rights used by one person.	Admin
Sponsored identity	User account used for example for training purposes.	Sponsored

Identity	Description	Value of the column "IdentityType"
Shared identity	User account with administration rights used by several people.	Shared
Service identity	Service account.	Service

- Privileged user account (column `IsPrivilegedAccount`)

  Use this option to flag user accounts with special, privileged permissions. This includes administrative user accounts or service accounts, for example. This option is not used to flag default user accounts.

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 manage level "Unmanaged" or "Full managed" to it.
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.

   An account definition specifies which rules are used to generate the IT operating data for example, whether the container for a user account is made up of the employee's department, cost center, location or business role and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

   - Use the default value "1" in the formatting rule for the column `IsGroupAccount` and set the option **Always use default value**.
   - Use the default value "primary" in the formatting rule for the column `IdentityType` and set the option **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, which 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.

Administrative User Accounts

An administrative user account must be used for certain administrative tasks. Administrative user accounts are normally predefined in the target system and have fixed identifiers and login names, for example, "Administrator".

Administrative user accounts are loaded through synchronization into the One Identity Manager. To assign a manager to administrative user accounts, assign an employee to the user account in One Identity Manager.

NOTE: You can automatically label administrative user accounts as privileged user accounts. To do this, set the schedule "Mark selected user accounts as privileged" in the Designer.

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 marked with the property **Privileged user account** (`IsPrivilegedAccount`).

NOTE: The criteria used to label user accounts automatically as privileged, are defined as extensions to the view definition (ViewAddOn) on the table `TSBVAccountIsPrivDetectRule` (table type "Union"). The evaluation is done in the script `TSB_SetIsPrivilegedAccount`.

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 properties for privileged user accounts being overwritten, set the property **IT operating data overwrites** for the manage level, to the value "Only initially". In this case, the properties are populated just once when the user accounts is created.
3. 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.
4. Create a formatting rule for IT operating data.

   An account definition specifies which rules are used to generate the IT operating data for example, whether the container for a user account is made up of the employee's department, cost center, location or business role and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

- Use the default value "1" in the formatting rule for the column `IsPrivilegedAccount` and set the option **Always use default value**.
- You can also specify a formatting rule for the column `IdentityType`. The column owns different permitted values, which represent user accounts.
- To prevent privileged user accounts inheriting default user groups, define a template for the column `IsGroupAccount` with the default value "0" and set the option **Always use default value**.

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.

NOTE: Specify a formatting rule for a naming schema if it is required by the company for privileged user account login names.

Entering Master Data for User Accounts

A user account can be linked to an employee in the 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 master data described in the following is mapped through templates from employee master data.

To edit master data for a user account

1. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list and run the task **Change master data**.

   - OR-

   Click in the result list toolbar.
3. Edit the user account's resource data.
4. Save the changes.

To manually assign or create a user account for an employee

1. Select the **Employees | Employees**.
2. Select the employee in the result list and run **Assign user accounts** from the task view.

3. Assign a user account.
4. Save the changes.

Related Topics

- User Account Master Data on page 67
- Linking User Accounts to Employees on page 62
- Supported User Account Types on page 63
- Setting Up Account Definitions on page 20

User Account Master Data

Enter the following data for a user account:

Table 25: 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.
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The 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.
Manage level	User account's manage level. 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	Target system in which the user account is created.
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

Property	Description
	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	User account's distinguished name. 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.
Risk index (calculated)	Maximum risk index values for all assigned groups. This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.
Category	Categories for the inheritance of groups by the user account. Select one or more categories from the menu. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories.
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, it will be used as the account expiry 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 expiry date remains intact!
Last login	Date of last target system login.
Password last changed	Data of last password change.
Password	Password for the user account. Depending on the configuration parameter "Person\UseCentralPassword" the employee's central password can be mapped to the user account's password. If you use an initial password for the user accounts, it is automatically entered when a user account is created.

Property	Description
	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.
Description	Spare text box for additional explanation.
Identity	User account's identity type

Table 26: Permitted values for the identity.

Value	Description
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 admin identity	User account with administrative permissions, used by one employee.
Sponsored identity	User account that is used for training purposes, for example.
Shared identity	User account with administrative permissions, used by several employees.
Service identity	Service account.

Privileged user account	Specifies whether this is a privileged user account.
Groups can be inherited	Specifies whether the user account groups can inherit through the employee. If this option is set, the user account inherits groups through hierarchical roles or 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. • 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.
User account is disabled	Specifies that 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 option <User account is deactivated>.

Related Topics

- Setting Up Account Definitions on page 20
- Password Policies on page 37
- Initial Password for New User Accounts on page 46
- Supported User Account Types on page 63
- Group Inheritance Based on Categories on page 89
- Disabling User Accounts on page 77

Additional Tasks for Managing User Accounts

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

Overview of User Accounts

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. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Select **User account overview** in the task view.

Changing the Manage Level of a User Account

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. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list.

3. Select **Change master data** in the task view.
4. Select the manage level in the **Manage level** menu on the tab **General**.
5. Save the changes.

Assigning Groups directly to User Accounts

Groups can be assigned directly or indirectly to a user account. Indirect assignment is carried out by allocating the employee and groups in hierarchical roles, like departments, cost centers, locations or business roles. If the employee has a user account in the target system, the groups in the role are inherited by this user account. You can assign groups to user accounts, which belong to the same target system or target system type.

To react quickly to special requests, you can assign groups directly to the user account.

To assign groups directly to user accounts

1. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Select **Assign groups** in the task view.
4. Assign groups in **Add assignments**.

   The view- OR -

   Remove groups from **Remove assignments**.
5. Save the changes.

Related Topics

- Target system types on page 52
- Assigning Group to User Accounts on page 81

Assigning Extended Properties

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

To specify extended properties for a user account

1. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Select **Assign extended properties** in the task view.

4. Assign extended properties in **Add assignments**.

   - OR -

   Remove assignments to extended properties in **Remove assignments**.
5. Save the changes.

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

Assigning Permissions Controls

Use this task to assign permissions controls directly to user accounts.

To assign permissions controls to a user account

1. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Select **Assign permissions controls**.
4. Assign permissions controls in **Add assignments**.

   - OR -

   Remove permissions controls from **Remove assignments**.
5. Save the changes.

Automatic Assignment of Employees to User Accounts

Table 27: Configuration Parameters for Automatic Employee Assignment

Configuration parameter	Meaning
TargetSys-tem\UNS\PersonAutoFullsync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSys-tem\UNS\PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSys-tem\UNS\PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names given in a pipe (|) delimited list that is handled as a regular search

Configuration parameter	Meaning
	pattern. Example: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.*\$`
TargetSystem\UNS\PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.

When you add a user account, an existing employee can be assigned automatically or added if necessary. In the process, the employee master data is created based for existing user master data. This mechanism can follow on after a new user account has been created 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 assignment 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 the task **Change master data** to assign employees to administrative user account for the respective user account.

Run the following tasks to assign employees automatically.

- If employees can be assigned by user accounts during synchronization, set the parameter "TargetSystem\UNS\PersonAutoFullsync" in the Designer and select the mode.
- If employees can be assigned by user accounts during synchronization, set the parameter "TargetSystem\UNS\PersonAutoDefault" in the Designer and select the mode.
- Specify the user accounts in the configuration parameter "TargetSystem\ADS\PersonExcludeList" which must not be assigned automatically to employees.

  Example:

  `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.*\$`
- Use the configuration parameter "TargetSystem\ADS\PersonAutoDisabledAccounts" 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 the manage level to be used is entered as default automation level.
- Define the search criteria for employees assigned to the target system.

  NOTE: You can populate the column `Person.ImportSource` in the script `TSB_PersonAuto_Mapping_UNSAccountB` to determine an employee's source. To do this, extend the list of values permitted in the column `Person.ImportSource` in the Designer and overwrite the script correspondingly.

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: Following synchronization, employees are automatically created for user accounts in the default installation. If there are no account definitions for the target system at the time of synchronization, user accounts are linked to employees. However, account definitions are not assigned. The user accounts are, therefore, in a "Linked" state.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the target system.
3. Assign the account definition and manage level to the user accounts in a "linked" state.
   a. Select the category **Custom target systems | <target system> | User accounts | Linked but not configured | <target system>**.
   b. Select the task **Assign account definition to linked accounts**.

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

Related Topics

- Creating an Account Definition on page 21
- Assigning an Account Definition to a Custom Target System on page 35
- Editing Search Criteria for Automatic Employee Assignment on page 75

Editing Search Criteria for Automatic Employee Assignment

Criteria for employee assignment are defined in the target systems. In this case, 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 criteria are written in XML notation in the column "Search criteria for automatic employee assignment" (`AccountToPersonMatchingRule`) of 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: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given 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.

It is not recommended to make assignment to administrative user accounts based on search criteria. Use the task **Change master data** to assign employees to administrative user account for the respective user account.

NOTE: One Identity Manager supplies a default mapping for employee assignment. Only carry out the following steps when you want to customize the default mapping.

To specify criteria for employee assignment

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

   Table 28: Default Search Criteria for User Accounts

Apply to	Column on Employee	Column on User Account user accounts
User accounts	Central user account (CentralAccount)	Login name (AccountName)

5. Save the changes.

Direct Assignment of Employees to User Accounts Based on a Suggestion List

You can create a suggestion list in the "Assignments" view for assignments of employees to user accounts based on the search criteria. User accounts are grouped in different views for this.

Table 29: 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.

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

To apply search criteria to user accounts

- Click **Reload**.

  All possible assignments based on the search criteria are found in the target system for all user accounts. The three views are updated.

To assign employees directly over a suggestion list

1. Click **Suggested assignments**.
   a. Click **Select** for all user accounts to be assigned to the suggested employee. Multi-select is possible.
   b. Click **Assign selected.**
   c. Confirm the security prompt with **Yes**.

      The selected user accounts are assigned to the employees found using the search criteria.

   – OR –
2. Click **No employee assignment**.
   a. Click **Select employee...** for the user account to which you want to assign the employee. Select an employee from the menu.
   b. Click **Select** for all user accounts to which you want to assign the selected employees. Multi-select is possible.

c. Click **Assign selected**.

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

This assigns the selected user accounts to the employees shown in the "Employee" column.

To remove assignments

1. Click **Assigned user accounts**.
   a. Click **Select** for all user accounts whose employee assignment you want to remove. Multi-select is possible.
   b. Click **Delete selected**.
   c. Confirm the security prompt with **Yes**.

   The assigned employees are deleted from the selected user accounts.

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

Related Topics

- Automatic Assignment of Employees to User Accounts on page 72

Disabling User Accounts

Table 30: Configuration Parameter for Disabling User Accounts

Configuration parameter	Meaning
QER\Person\TemporaryDeactivation	This configuration parameter specifies whether user accounts for an employee are locked if the employee is temporarily or permanently disabled.

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

Scenario:

- The user account is linked to employees and is 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. User accounts with the manage level "Full managed" are disabled depending on the account definition settings. For user accounts with another manage level, modify the column template `UNSAccountB.AccountDisabled` accordingly.

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 configuration parameter "QER\Person\TemporaryDeactivation".

- If the configuration parameter is set, the employee's user accounts are disabled if 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 lock a user account when the configuration parameter is disabled

1. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Account is disabled** on the **General** tab.
5. Save the changes.

Scenario:

- User accounts not linked to employees.

To lock a user account, which is not linked to an employee

1. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.
4. Set the option **Account is disabled** on the **General** tab.
5. Save the changes.

For more detailed 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 78
- Creating an Account Definition on page 21
- Setting Up Manage Levels on page 24

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 created through this account definition, is deleted.

You can delete a user account, which 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 finally deleted from the database and the One Identity Manager depending on the deferred deletion setting.

Configuring Deferred Deletion

By default, user accounts are finally deleted from the database after 30 days. During this period you have the option to reactivate the user accounts. A restore is not possible once the delete delay has expired. You can configure an alternative delay on the table ADSAccount in the Designer.

To delete a user account

1. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Click in the result list toolbar.
4. Confirm the security prompt with **Yes**.

To restore user account

1. Select the category **Custom target systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Click **Undo delete** in the result list toolbar.

Related Topics

- Disabling User Accounts on page 77

Groups in a Custom Target System

Groups map the objects that control access to target system resources in the target systems. A user receives access to target system resources through group memberships and access permissions.

To edit group master data

1. Select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list and run **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Edit a group's master data.
4. Save the changes.

Detailed information about this topic

- Group Master Data on page 80

Group Master Data

Enter the following master data for a group.

Table 31: Entering Master Data for a Group

Property	Description
Name	Group name.
Canonical name	The canonical name is generated automatically and should not be changed.
Distinguished name	The distinguished name is determined using a template and must not be changed.

Property	Description
Display name	The display name is used to display the group in the One Identity Manager tools user interface.
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. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. For more detailed 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. Use this menu to allocate one or more categories to the group.
Description	Spare text box for additional explanation.
IT Shop	Specifies whether the group can be requested through the IT Shop. This group can be requested by staff through the Web Portal and granted through a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. This group can be requested by staff through the Web Portal and granted through a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is no permitted.

Related Topics

- Group Inheritance Based on Categories on page 89
- For more detailed information about preparing groups for requesting through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Assigning Group to User Accounts

Groups can be assigned directly or indirectly to user accounts. In the case of indirect assignment, employees and groups are assigned to hierarchical roles, such as , departments, cost centers, locations or business roles. The groups assigned to an employee are calculated from the position in the hierarchy and the direction of inheritance.

If you add an employee to roles and that employee owns a user account in a target system, the user account is added to the group. Prerequisites for indirect assignment of employees to user accounts:

- Direct assignment of employees and groups of custom target systems is permitted for role classes (department, cost center, location or business role).
- The user accounts are marked with the option **Groups can be inherited**.

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

For more detailed information about inheriting company resources, see the One Identity Manager Identity Management Base Module Administration Guide.

Related Topics

- Target system types on page 52

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. Select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.
   - Assign departments on the **Departments** tab.
   - Assign locations on the **Locations** tab.
   - Assign cost centers on the **Cost center** tab.

   - OR -

   Remove the organizations from **Remove assignments**.
5. Save the changes.

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

1. Select the category **Organizations | Departments**.

   - OR -

   Select the category **Organizations | Cost centers**.

   - OR -

Select the category **Organizations | Locations**.

2. Select the department, cost center or location in the result list.
3. Select **Assign custom target system groups.**
4. Assign groups in **Add assignments**.

   - OR -

   Remove assignments to groups in **Remove assignments**.
5. Save the changes.

Assigning Groups to Business Roles

Installed Module: Business Roles Module

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. Select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

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

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

1. Select the category **Business roles | <Role class>**.
2. Select the business role in the result list.
3. Select **Assign custom target system groups.**
4. Assign groups in **Add assignments**.

   - OR -

   Remove assignments to groups in **Remove assignments**.
5. Save the changes.

Assigning User Accounts to a Group

Groups can be assigned directly or indirectly to a user account. Indirect assignment is carried out by allocating the employee and groups in hierarchical roles, like departments, cost centers, locations or business roles. If the employee has a user account in the target system, the groups in the role are inherited by this user account. You can assign groups to user accounts, which belong to the same target system or target system type.

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

To assign a group directly to user accounts

1. Select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign user accounts** in the task view.
4. Assign user accounts in **Add assignments**.

   The view- OR -

   Remove user accounts from **Remove assignments**.
5. Save the changes.

Add Groups to System Roles

Installed Modules: System Roles Module

Use this task to add a group to system roles. If you assign a system role to employees, all the employees' user accounts inherit the group.

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

To assign a group to system roles

1. Select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign system roles in the task view**.
4. Assign system roles in **Add assignments**.

   - OR -

   Remove system roles from **Remove assignments**.
5. Save the changes.

Adding Groups to the IT Shop

Once a group has been assigned 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 option **IT Shop**.
- The group must be assigned to a service item.
- The group must be labeled with the option **Only use in IT Shop** if the group can only be assigned to employees through IT Shop requests. Direct assignment to hierarchical roles or user accounts is no longer permitted.

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

To add a group to the IT Shop

1. Select the category **Custom Target Systems | <target system> | Groups** (non role-based login).

   - OR -

   Select the category **Entitlements | Groups** (role-based login).
2. Select the group in the result list.
3. Select **Add to IT Shop** in the task view.
4. Assign the group to the IT Shop shelves in **Add assignments**.
5. Save the changes.

To remove a group from individual IT Shop shelves.

1. Select the category **Custom Target Systems | <target system> | Groups** (non role-based login).

   - OR -

   Select the category **Entitlements | Groups** (role-based login).
2. Select the group in the result list.
3. Select **Add to IT Shop** in the task view.
4. Remove the group from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove a group from all IT Shop shelves.

1. Select the category **Custom Target Systems | <target system> | Groups** (non role-based login).

   - OR -

   Select the category **Entitlements | Groups** (role-based login).

2. Select the group in the result list.
3. Select **Remove from all shelves (IT Shop)** in the task view.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

   This removes the group from all One Identity Manager Service shelves. All requests and assignment requests with this group are canceled in the process.

For more detailed information about request from company resources through the IT Shop, see the One Identity Manager IT Shop Administration Guide.

Related Topics

- Group Master Data on page 80

Additional Tasks for Managing Groups

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

Overview of Groups

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

To obtain an overview of a group

1. Select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Group overview** in the task view.

Adding Groups to Groups

Use this task to add a group to another group. Only groups from the same target system can be assigned.

To assign groups directly to a group

1. Select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign groups** in the task view.

4. Assign child groups of the selected group in **Add assignments**.

   - OR -

   Remove assignments to groups in **Remove assignments**.
5. Save the changes.

Effectiveness of Group Memberships

Table 32: Configuration Parameter for Conditional Inheritance

Configuration parameter	Active Meaning
QER\Structures\Inherite\GroupExclusion	Preprocessor relevant configuration parameter for controlling effectiveness of group memberships. If the parameter is set, memberships can be reduced on the basis of exclusion definitions. The database has to be recompiled after changes have been made to the parameter.

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 directly, indirectly or by IT Shop request at any time. 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 whether membership of an excluded group is permitted in another group.

The effect of the assignments is mapped in the tables UNSAccountBInUNSGroupB and BaseTreeHasUNSGroupB through the column XIsInEffect.

Example of 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 department "Marketing", group B through "Finance" and group C through the business role "Control group".

Clara Harris has a user account in this target system. She primarily belongs to the department "marketing". The business role "Control group" and the department "Finance" are assigned to her 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 33: Specifying excluded groups (table `UNSGroupBExclusion`)

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

Table 34: Effective Assignments

Employee	Member in Role	Effective Group
Ben King	Marketing	Group A
Jan Bloggs	Marketing, finance	Group B
Clara Harris	Marketing, finance, control group	Group C
Jenny Basset	Marketing, control group	Group A, Group C

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

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

Table 35: Excluded groups and effective assignments

Employee	Member in Role	Assigned Group	Excluded Group	Effective Group
Jenny Basset	Marketing	Group A		Group C
	Control group	Group C	Group B	
			Group A	

Prerequisites

- The configuration parameter "QER\Inherite\GroupExclusion" is enabled.
- Mutually exclusive groups belong to the same target system or the same target system type.

NOTE: Groups, which 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. Select the category **Custom target systems | <target system> | Groups**.
2. Select a group in the result list.
3. Select **Exclude groups** in the task view.
4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.

   - OR -

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

Group Inheritance Based on Categories

In One Identity Manager, groups can be selectively inherited by user accounts. For this, groups and user accounts are divided into categories. The categories can be freely selected and are specified by a template. Each category is given a specific position within the template. The template contains two tables; the user account table and the group table. Use the user account table to specify categories for target system dependent user accounts. Enter your categories for the target system dependent groups, administrative roles, subscriptions and disabled service plans in the . Each table contains the category items "Position1" to "Position31".

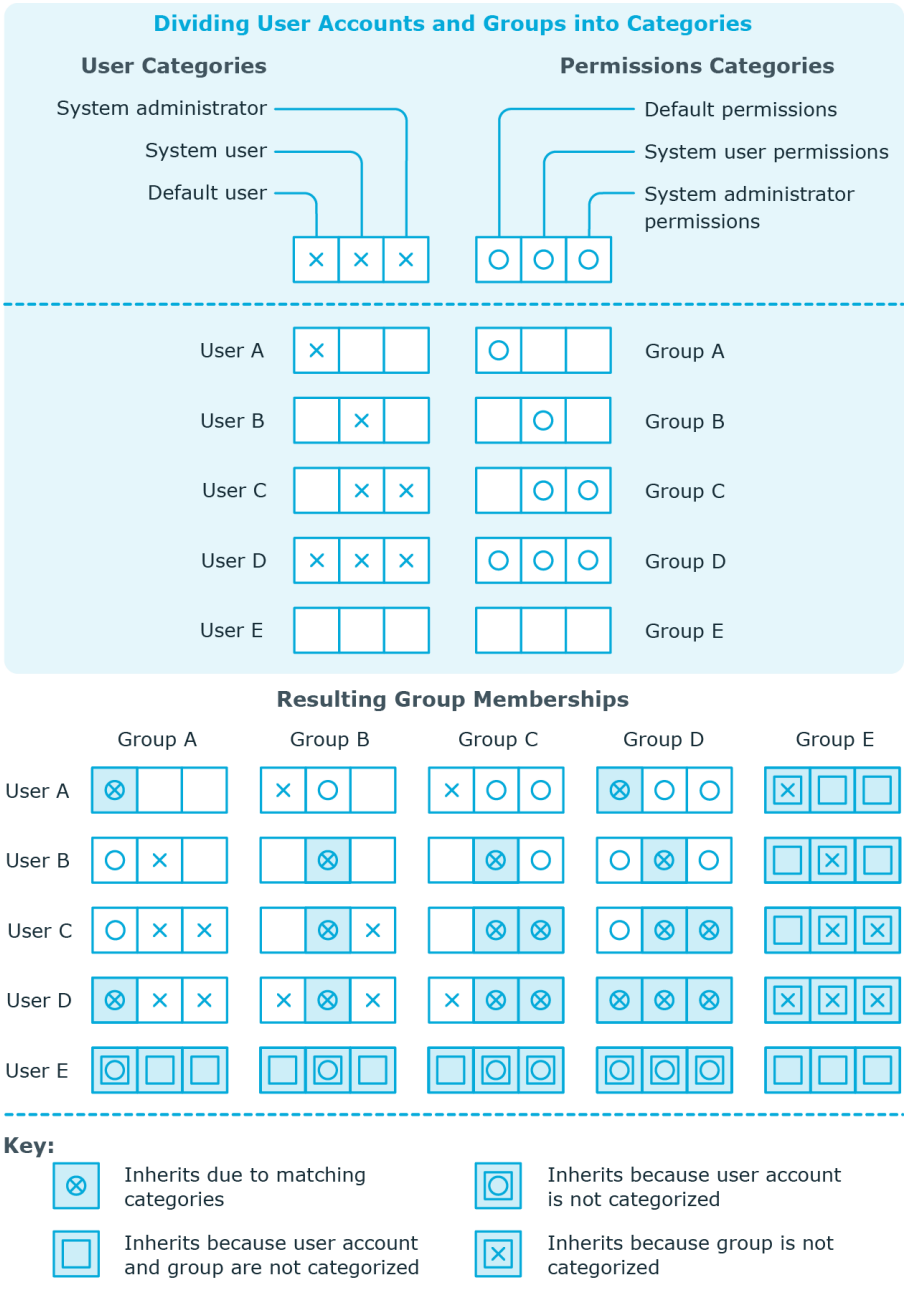
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category item matches an assigned group. The group is also inherited by the user account if the group or the 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 36: Category Examples

Category Position	Categories for User Accounts	Categories for Groups
1	Default user	Default permissions
2	System user	System user permissions
3	System administrator	System administrator permissions

Figure 1: Example of inheriting through categories.



To use inheritance through categories

- Define categories in the target system.
- Assign categories to user accounts through their master data.
- Assign categories to groups through their master data.

Related Topics

- Specifying Categories for Inheriting Groups on page 58
- User Account Master Data on page 67
- Group Master Data on page 80

Assigning Extended Properties

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

To specify extended properties for a group

1. Select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   The view- OR -

   Remove extended properties from **Remove assignments**.
5. Save the changes.

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

Assigning Permissions Controls

Use this task to assign permissions controls to groups.

To assign permissions controls to a group

1. Select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign permissions controls**.
4. Double-click on the permission controls you want to assign in **Add assignments**.

   - OR -

Double-click on the permissions controls in **Remove assignments** to remove their assignments.

5. Save the changes.

Related Topics

- Entering Permissions Controls on page 93

Entering Permissions Controls

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

To edit permissions controls

1. Select the category **Custom target systems | <target system> | Permissions controls**.
2. Select a permissions control in the result list. Select **Change master data** in the task view.

   - OR -

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

Detailed information about this topic

- Permissions Control Master Data on page 93

Permissions Control Master Data

Enter the following master data for a permissions control.

Table 37: Permissions Control Master Data

Property	Description
Target System	Target system in which the permissions control applies.
Permissions control	Name of the permissions control.
Access type	Additional permissions control properties.

Property	Description
Description	Spare text box for additional explanation.
Spare fields no. 01.....spare field no. 10	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Additional Tasks for Permissions Controls

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

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. Select the category **Custom target systems | <target system> | Permissions controls**.
2. Select the permissions control in the result list.
3. Select **Permissions control overview** in the task view.

Assigning Permissions Controls to User Accounts

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

To assign permissions controls to user accounts

1. Select the category **Custom target systems | <target system> | Permissions controls**.
2. Select the permissions control in the result list.
3. Select **Assign user accounts** in the task view.
4. Assign user accounts in **Add assignments**.

The view- OR -

Remove user accounts from **Remove assignments**.

5. Save the changes.

Assigning Permissions Controls to Groups

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

To assign groups to a permissions control

1. Select the category **Custom target systems | <target system> | Permissions controls**.
2. Select the permissions control in the result list.
3. Select **Assign groups** in the task view.
4. Assign groups in **Add assignments**.

   The view- OR -

   Remove groups from **Remove assignments**.
5. Save the changes.

9

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 38: Reports for the Target System

Report	Description
Overview of all assignments (target system)	This report finds all roles containing employees with at least one user account in the selected target system.
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 (group)	This report finds all roles containing employees with the selected group.
Show orphaned user accounts	This report shows all user accounts in the target system which are not assigned an employee.
Show employees with multiple user accounts	This report shows all employees with more than one user account in the target system.
Show unused user accounts	This report shows all user accounts in the target system that have not been used in the last few months.
Show entitlement drifts	This report shows all target system groups, which are the result of manual operations in the target system rather than provisioned through One Identity Manager.
Show user accounts with an above average number of system entitlements	This report contains all user accounts in the target system with an above average number of group memberships.

Related Topics

- Overview of all Assignments on page 97

Overview of all Assignments

The report "Overview of all Assignments" is displayed for certain objects, for example, permissions, compliance rules or roles. The report finds all the roles, for example, departments, cost centers, locations, business roles and IT Shop structures in which there are employee who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Example

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

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the report **Overview of all assignments**.
- Use the **Used by button** in the report's toolbar to select the role class (department, location, business role or IT Shop structure) for which you determine if roles exist in which there are employees with the selected base object.

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. In the report's toolbar, click to open the legend.
- Double-click a control to show all child roles belonging to the selected role.
- By clicking the button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to to start a wizard that allows you to bookmark this list of employee for tracking. This creates a new business role to which the employees are assigned.

Figure 2: Toolbar for Report "Overview of all assignments"

Table 39: 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.

A

Appendix: 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 40: Configuration Parameters for Managing Custom Target Systems

Configuration parameter	Meaning
TargetSystem\UNS	Preprocessor relevant configuration parameter to control the component parts for the managing custom target systems. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.
TargetSystem\UNS\Accounts	This configuration parameter permits configuration of user account data.
TargetSystem\UNS\Accounts\ InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. It must contain at least those character sets set in the configuration subparameters.
TargetSystem\UNS\Accounts\ InitialRandomPassword\SendTo	This configuration parameter specifies to which employee the email with the random generated password should be sent (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	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account). Use the

Configuration parameter	Meaning
	mail template "Employee - new account created".
TargetSystem\UNS\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password). Use the mail template "Employee - initial password for new user account".
TargetSystem\UNS\Accounts\MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. Use the mail template "Employee - new user account with default properties created".
TargetSystem\UNS\CreateNewRoot	The configuration parameter specifies whether new target systems can be added. If this parameter is set, custom target systems can be added.
TargetSystem\UNS\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem\UNS\PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\UNS\PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.
TargetSystem\UNS\PersonAutoFullSync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\UNS\PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names given 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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

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

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

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

Index

A

account definition 20
- add to IT Shop 34
- assign to system roles 33

C

configuration parameter 99
custom target system 6
- account definition 20
  - assign automatically 32
  - assign to all employees 32
  - assign to business role 31
  - assign to cost center 31
  - assign to department 31
  - assign to employee 30, 33
  - assign to location 31
  - create 21
  - delete 36
  - IT operating data 26-27
  - manage level 24
- container 60
- group 80
  - assign extended properties 91
  - assign group 86
  - assign permissions element 91
  - assign system role 84
  - assign to business role 83
  - assign to cost center 82
  - assign to department 82
  - assign to location 82
  - assign to user account 71, 81, 84
  - category 80, 89
  - edit 80
  - effective 87
  - exclusion 87
  - pass down 81, 89
  - risk index 80
  - target system type 52

permissions control 93
- assign group 91, 95
- assign user account 72, 94

provisioning by script 9-10
- server 11

report 96
target system
- account definition 35, 56
- alternative column description 59
- category 58
- display name 56
- edit 55
- no write operations 58
- synchronization by script 56
- synchronization server 11, 58
- synchronized by 56
- target system managers 56
- target system type 56

target system administrator 6
target system manager 6, 49, 56
target system type 52
- cross boundary inheritance 52
- group membership 52

user 6

user account 62
account definition 67
administrative user account 63
assign employee 62, 72
assign extended properties 71
assign group 71
assign permissions control 72
category 67, 89
default user accounts 63
delete 78
disable 77
edit 66
identity 63, 67
inherit group 67
login name 67
manage level 67, 70
password 67
initial 46
privileged user account 63, 67
restore 78
type 63

E

email notification 48
employee assignment
automatic 72
manual 76
remove 76
search criteria 75
table column 75

I

IT operating data
change 29
IT Shop shelf
assign account definition 34

L

login data 48

N

notification 48

O

object
delete immediately 16
outstanding 15-16
publish 16
outstanding object 15

P

password
initial 48
password policy 37
assign 45
character sets 40
check password 44
conversion script 41, 43
default policy 39, 45
display name 39
edit 39
error message 39
excluded list 44
failed logins 40
generate password 44
initial password 40
name components 40

password age 40
password cycle 40
password length 40
password strength 40
predefined 38
test script 41

T

target system
overview of all assignments 97
target system synchronization
table to assign 16
target system type 16
template
IT operating data, modify 29

U

user account
administrative user account 63
apply template 29
default user accounts 63
identity 63
password
notification 48
privileged user account 63
type 63