One Identity Manager 8.1

Administration Guide for Connecting to Custom Target Systems

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 2019
Version - 8.1

Contents

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: Users

Users	Task
Target system admin-	Target system administrators must be assigned to the **Target**

Users	Task
istrators	**systems | Administrators** application role. 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	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. • Can create employees with an identity that differs from the **Primary identity**. • 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 Designer as required. • Create system users and permissions groups for non-role-based login to administration tools in Designer as required. • Enable or disable additional configuration parameters in Designer as required. • Create custom processes in Designer as required.

Users	Task
	• Create and configures schedules as required. • Create and configure password policies as required.
Administrators for the IT Shop	Administrators must be assigned to the **Request & Fulfillment | IT Shop | Administrators** application role. Users with this application role: • Assign groups to IT Shop structures.
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:

- Creating scripts for provisioning

  The data from One Identity Manager is provisioned to a custom target system using scripts. These must be created for each target system. For more information, see Creating the scripts for data provisioning in a custom target system on page 11.

- Preparing a server for provisioning

  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 to a custom target system on page 12.

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

  Select "Synchronization by script". For more information, see Setting up a custom target system on page 57.

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 scripts for data provisioning in a custom target system

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

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

Create custom scripts for your target system. You can use the 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 "Telephone system" target system

`CCC_UNSAccountB_Telephonesystem_Insert`

IMPORTANT: If your target system contains a hyphen ("-") in its name, you must remove it from the script function in the 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 to 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 Manager.
    a. Select **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 12
- Customizing data synchronization for a custom target system on page 59
- 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 also available in Designer under **Base Data | Installation | Job server**.

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

Table 3: Job Server Properties

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

Property	Meaning
system	
Language	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The 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. At present, only copy methods that support the Robocopy and rsync programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the Robocopy program between servers with a Windows operating system or with the rsync program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the 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.

Property	Meaning
Queue	Name of the queue to handle the process steps. Each One Identity Manager 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. The values **Win32**, **Windows**, **Linux** and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server) the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the 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 the program "Job Queue Info". For more detailed information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update 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 14

Specifying server functions

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

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

Table 4: Permitted server functions

Server function	Remark
CSV connector	Server on which the CSV connector for synchronization is installed.
Domain controller	The Active Directory domain controller. Servers that are not labeled as domain 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 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	The server can execute 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.
CSV script server	The server can process CSV files using the `ScriptComponent` process component.
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.

Server function	Remark
SAM synchronization Server	Server for running synchronization with an SMB-based target system.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Windows PowerShell connector	The server can run Windows PowerShell version 3.0 or later.

Post-processing outstanding objects

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

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

Outstanding objects

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

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

Start target system synchronization to do this.

To allow post-processing of outstanding objects

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

  For more information, see Configuring target system synchronization on page 17.

Related Topics

- Target system types on page 53
- Post-processing outstanding objects on page 18

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

To add tables to the target system synchronization

1. In the result list, select the target system type of the custom-defined target system.
2. Select **Assign synchronization tables**.
3. Assign tables whose outstanding objects you want to handle in **Add assignments**.
4. Save the changes.
5. Select **Configure tables for publishing**.
6. Select tables whose outstanding objects can be published in the target system and set **Publishable**.
7. Save the changes.

To publish outstanding objects

- For each table for which you want to publish outstanding objects, create a process, which is triggered by the event `HandleOutstanding` and which executes the provisioning of the objects. Use the `AdHocProjection` process function of the `ProjectorComponent` process component. For detailed information about defining processes, see the *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 10.

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 detailed information, see the *One Identity Manager Target System Synchronization Reference Guide*.

Post-processing outstanding objects

To post-process outstanding objects

1. Select **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 database. Deferred deletion is not taken into account. The **Outstanding** label is removed for the object. Indirect memberships cannot be deleted.
	Publish	The object is added in the target system. The **Outstanding** label is removed for the object. The method triggers the `HandleOutstanding` event. This runs a target system specific process that triggers the provisioning process for the object. Prerequisites: • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The **Outstanding** label is removed for the object.

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

NOTE: By default, the selected objects are processed in parallel, which speeds up 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 17

3

Basic data for custom target systems

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

- Configuration parameters

  Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for 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 **Base data | General | Configuration parameters** in Designer.

  For more information, see Appendix: Configuration parameters for managing custom target systems on page 105.

- 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 yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

  For more information, see Setting up account definitions on page 21.

- 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 for user accounts on page 39.

- 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 49.

- 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 50.

- 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 to a custom target system on page 12.

- Target system managers

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

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

  For more information, see Target system managers on page 51.

- 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 53.

- 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 custom schema extensions for custom target systems on page 54.

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 yet have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee.

The data for the user accounts in the respective target system comes from the basic employee data. The employees must have a user account. The assignment of the IT operating data to the employee's user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role (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. In the Manager, 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**.

   - 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 22

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 that 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 input field is only visible if the configuration parameter **QER | CalculateRiskIndex** is activated. 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 also be assigned directly to employees and roles outside of 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 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.

One Identity Manager supplies a default configuration for manage levels:

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

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

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

Specify the effect of temporarily or permanently disabling, deleting or the security risk of an employee on its user accounts and group memberships for each manage level.

- 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. In the Manager, 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**.

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

   - OR -

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

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

To edit a manage level

1. Select **Custom Target Systems | Basic configuration data | Account definitions | Manage levels**.
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 26

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**: The data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.

Property	Description
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. In the Manager, 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** 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. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template.
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. The **Employee - new user account with default properties created** mail template is used. To change the mail template, adjust the **TargetSystem | UNS | Accounts | MailTemplateDefaultValues** configuration parameter.

4. Save the changes.

Related Topics

- Determining IT operating data on page 28

Determining IT operating data

To create user accounts with the **Full managed** manage level, the required 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 domainA. In addition, certain employees in department A obtain administrative user accounts in the domainA.

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 define IT operating data

1. In Manager, select the role in the **Organizations** or **Business roles** category.
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. Under **Table**, select the table that maps the target system for select the `TSBAccountDef` table for an account definition. c. Select the specific target system or account definition under **Effects on**.

Property	Description
	d. Click **OK**.
Column	User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template.
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 27

Modify 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 effect a change to the IT operating data has on the existing user accounts. You can decide whether the change is transferred to the One Identity Manager database in the case of each affected column in each affected database.

Prerequisites

- The IT operating data of a department, 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. In the Manager, 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:	Value that the object property would have following modification of the IT operating data.
Selection:	Specifies whether the modification shall be adopted for 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).

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 assignment of an account definition is removed, the user account that was created from this account definition is.

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 32
- Assigning account definitions to business roles on page 33
- Assigning account definitions to all employees on page 33
- Assigning account definitions directly to employees on page 34
- Assigning an account definition to a custom target system on page 37

Assigning account definitions to departments, cost centers, and locations

To add account definitions to hierarchical roles

1. In the Manager, 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 centers** tab.

   TIP: In the **Remove assignments** area, you can remove the assignment of organizations.

   To remove an assignment

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

Related Topics

- Assigning account definitions to business roles on page 33
- Assigning account definitions to all employees on page 33
- Assigning account definitions directly to employees on page 34

Assigning account definitions to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

1. In the Manager, 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**.
4. Assign business roles in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of business roles.

   To remove an assignment

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

Related Topics

- Assigning account definitions to departments, cost centers, and locations on page 32
- Assigning account definitions to all employees on page 33
- Assigning account definitions directly to employees on page 34

Assigning account definitions to all employees

To assign an account definition to all employees

1. In the Manager, 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**.

4. Set **Automatic assignment to employees** on **General**.

   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 **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 32
- Assigning account definitions to business roles on page 33
- Assigning account definitions directly to employees on page 34

Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In the Manager, 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**.
4. Assign employees in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of employees.

   To remove an assignment

   - Select the employee and double click ✓.

5. Save the changes.

Related Topics

- Assigning account definitions to departments, cost centers, and locations on page 32
- Assigning account definitions to business roles on page 33
- Assigning account definitions to all employees on page 33

Assigning account definitions to system roles

Installed modules: System Roles Module

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

To add account definitions to a system role

1. In the Manager, select the 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**.
4. Assign system roles in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of system roles.

   To remove an assignment

   - Select the system role and double click ✓.
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.

  TIP: In Web Portal, all products that can be requested are grouped together by service category. To make the account definition easier to find in Web Portal, assign a service category to the service item.
- If the account definition is only assigned to employees using IT Shop assignments, you must also set **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. In Manager, select **Custom Target Systems | Basic configuration data | Account definitions | Account definitions** (non-role-based login).

   - OR -

   In Manager, select **Entitlements | Account definitions** (role-based login).
2. Select an account definition in the result list.
3. Select **Add to IT Shop**.
4. Assign the account definitions to the IT Shop shelves in **Add assignments**.
5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. In Manager, select **Custom Target Systems | Basic configuration data | Account definitions | Account definitions** (non-role-based login).

   - OR -

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

To remove an account definition from all IT Shop shelves

1. In Manager, select **Custom Target Systems | Basic configuration data | Account definitions | Account definitions** (non-role-based login).

   - OR -

   In the Manager, select **Entitlements | Account definitions** (with role-based login).
2. Select an account definition in the result list.
3. Select **Remove from all shelves (IT Shop)**.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

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

Related Topics

- Master data for an account definition on page 22
- Assigning account definitions to departments, cost centers, and locations on page 32
- Assigning account definitions to business roles on page 33
- Assigning account definitions directly to employees on page 34
- Assigning account definitions to system roles on page 35

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 (**Linked**) if no account definition is given.

To assign the account definition to a target system

1. In Manager, select the target system in **Custom target systems**.
2. Select **Change master data**.
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 77

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.

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.
    a. In the Manager, 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**.
    d. Disable **Automatic assignment to employees** on the **General** tab.
    e. Save the changes.
2. Remove direct assignments of the account definition to employees.
    a. In the Manager, 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**.
    d. Remove employees from **Remove assignments**.
    e. Save the changes.
3. Remove the account definition's assignments to departments, cost centers and locations.
    a. In the Manager, 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. In **Remove assignments**, remove the relevant departments, cost centers, and locations.
    e. Save the changes.
4. Remove the account definition's assignments to business roles.
    a. In the Manager, select the 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**.

        Remove the business roles in **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 about unsubscribing requests, see the *One Identity Manager Web Portal User Guide*.

To remove an account definition from all IT Shop shelves

a. In Manager, select **Custom Target Systems | Basic configuration data | Account definitions | Account definitions** (non-role-based login).

   - OR -

   In the Manager, select **Entitlements | Account definitions** (with role-based login).

b. Select an account definition in the result list.

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

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

e. Click **OK**.

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

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. In the Manager, 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**.

   d. Remove the account definition in the **Required account definition** menu.

   e. Save the changes.

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

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

   b. Select **Change master data**.

   c. Remove the assigned account definitions on the **General** tab.

   d. Save the changes.

8. Delete the account definition.

   a. In the Manager, 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 an account definition.

Password policies for user accounts

One Identity Manager provides you with support for creating complex password policies, for example, for system user passwords, the employees' central password as well as

passwords for individual target systems. Password polices apply not only when the user enters a password but also when random passwords are generated.

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

Detailed information about this topic

- Predefined password policies on page 40
- Editing password policies on page 43
- Custom scripts for password requirements on page 46
- Excluded list for passwords on page 48
- Checking a password on page 49
- Testing generation of a password on page 49
- Using a password policy on page 41

Predefined password policies

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

Password for logging in to One Identity Manager

The **One Identity Manager password policy** is applied for logging in to One Identity Manager. This password policy 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`).

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

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

Password policy for forming employees' central passwords

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

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

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

Password policies for user accounts

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

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

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

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

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

Using 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.

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

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

1. Password policy of the account definition of the user account
2. Password policy of the manage level of the user account
3. Password policy **One Identity Manager password policy** (default policy)

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

To reassign a password policy

1. Select **Custom target systems | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Assign objects**.
4. Click **Add** in the **Assignments** section and enter the following data.

Table 10: 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 one of the following references under **Table**: • The table that contains the base objects of synchronization. • Select the `TSBAccountDef` table to apply the password policy based on the account definition. • Select the `TSBBehavior` table to apply the password policy based on the manage level. c. Select the table that contains the base objects under **Apply to**. • If you have selected the table containing the base objects of synchronization, next select the specific target system. • If you have selected the `TSBAccountDef` table, next select the specific account definition. • If you have selected the `TSBBehavior` table, next select the specific manage level. 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 **Custom target systems | Basic configuration data | Password policies** in Manager.
2. Select the password policy in the result list.
3. Select **Assign objects**.
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.

Editing password policies

To edit a password policy

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

   - 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 43
- Policy settings on page 44
- Character classes for passwords on page 45
- Custom scripts for password requirements on page 46

General master data for a password policy

Enter the following master data for a password policy.

Table 11: 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.

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

Policy settings

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

Table 12: Policy Settings

Property	Meaning
Initial password	Initial password for newly created user accounts. If a password is not entered or if a random password is not generated when a user account is created, the initial password is used.
Password confirmation	Reconfirm password.
Max. 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. Only taken into account when logging in to One Identity Manager. If a user has reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager. You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. For more detailed information, see the *One Identity Manager Web Portal User Guide*.
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, for example, a value of **5** is entered, the user's last five passwords are stored.
Min. password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3**

Property	Meaning
	and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted or not permitted in the password. If this option is enabled, name properties are not permitted in passwords. The values of the columns for which the **Contains name properties for password check** option is set are taken into account. Adjust this option in the column definition in Designer.

Character classes for passwords

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

Table 13: Character classes for passwords

Property	Meaning
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted characters.
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.
Denied special characters	List of characters, which are not permitted.
Lowercase not allowed	Specifies whether the password can contain lower case letters. This setting is only applies when passwords are generated.

Property	Meaning
Uppercase not allowed	Specifies whether the password can contain upper case letters. This setting is only applies when passwords are generated.
Digits not allowed	Specifies whether the password can contain digits. This setting is only applies when passwords are generated.
Special characters not allowed	Specifies whether the password can contain special characters. This setting is only applies when passwords are generated.

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 46
- Script for generating a password on page 47

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 start with **?** or **!**. 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 **Custom target systems | Basic configuration data | Password policies** in Manager.
    b. Select the password policy in the result list.
    c. Select **Change master data**.
    d. Enter the name of the script to be used to check a password in the **Check script** input field on the **Scripts** tab.
    e. Save the changes.

Related Topics

- Script for generating a password on page 47

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

In random passwords, the script replaces the **?** and **!** characters, which are not permitted.

```
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 **Custom target systems | Basic configuration data | Password policies** in Manager.
    b. Select the password policy in the result list.
    c. Select **Change master data**.
    d. Enter the name of the script to be used to generate a password in the **Generating script** input field on the **Scripts** tab.
    e. Save the changes.

Related Topics

- Script for checking a password on page 46

Excluded list for 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 **Base Data | Security settings | Restricted passwords** in Designer.
2. Create a new entry with **Object | New** an enter the term to excluded to the list.

3. Save the changes.

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

   This generates and displays a password.

Initial password for new user accounts

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

- Create user accounts manually and enter a password in their master data.
- Assign a randomly generated initial password to enter when you create user accounts.
  - Enable the **TargetSystem | UNS| Accounts | InitialRandomPassword** configuration parameter in 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.
- User the employee's central password. The employee's central password is mapped to the user account password. For detailed information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*.

Related Topics

- Password policies for user accounts on page 39
- Email notifications about login data on page 50

Email notifications about login data

You can configure the login information for new user accounts to be sent by email to a specified person. In this case, two messages are sent with the user name and the initial password. Mail templates are used to generate the messages. The mail text is defined in several languages in a mail template. 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.

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

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

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

   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

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

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

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

Implementing application roles for target system managers

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

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

Table 14: Default Application Roles for Target System Managers

Users	Tasks
target system managers	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. • Can create employees with an identity that differs from the **Primary identity**. • 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 One Identity Manager as Manager administrator (**Base role | Administrators**)
2. Select **One Identity Manager Administration | Target systems | Administrators**.
3. Select **Assign employees**.
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 Manager as target system administrator (**Target systems | Administrators**).
2. Select **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 Manager as target system manager.
2. Select the application role in **Custom Target Systems | Basic configuration data | Target system managers**.

3. Select **Assign employees**.
4. Assign the employees you want and save the changes.

1. Login to 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**.
5. On the **General** tab, select the application role in the **Target system manager** menu.

   - OR -

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

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

   b. Click **OK** to add the new application role.
6. Save the changes.

Related Topics

- One Identity Manager users for managing custom target systems on page 7
- General master data for a custom target system on page 58

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 16.

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

Displaying custom schema extensions 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.

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

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

Example

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

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

Table 16: 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 17: 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**.

   - 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 **Custom target systems | <target system>**.

Detailed information about this topic

- General master data for a custom target system on page 58
- Customizing data synchronization for a custom target system on page 59

- Specifying categories for inheriting groups on page 60
- Alternative column names on page 61

General master data for a custom target system

Enter the following data for a custom target system.

Table 18: 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. This account definition is used if automatic assignment of employees to user accounts is used for this and if user accounts are to be created that are already managed (**Linked configured**). The account definition's default manage level is applied. User accounts are only linked to the employee (**Linked**) if no account definition is given. This is the case on initial synchronization, for example.
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.

Property	Description
	Select the One Identity Manager application role whose members are responsible for administration of this target system. Use the button to add a new application role.
Synchronized by	Type of synchronization through which the data is synchronized between the target system and One Identity Manager. As soon as objects for this target system are available in One Identity Manager, the type of synchronization can no longer be changed. **Table 19: Permitted values** **Value** / **Synchronization by** / **Provisioned by** Synchronization by script / none / One Identity Manager script components No synchronization / none / none If you select **Scripted synchronization**, 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 53
- Automatic assignment of employees to user accounts on page 77
- Target system managers on page 51

Customizing data synchronization for a custom target system

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 20: 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 to a custom target system on page 12

Specifying categories for inheriting groups

In One Identity Manager, groups can be selectively inherited by user accounts. For this purpose, the groups and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within this mapping rule. 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. In the group table enter your categories for the target system-dependent groups. Each table contains the category positions **Position 1** to **Position 31**.

To define a category

1. In Manager, select the target system in **Custom target systems**.
2. Select **Change master data**.
3. Switch to the **Mapping rule category** tab.
4. Extend the relevant roots of the user account table or group table.
5. Click to enable category.
6. Enter a category name of your choice for user accounts and and in the login language used.
7. Save the changes.

Detailed information about this topic

- Group inheritance based on categories on page 95

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. In the result list, select a target system. Select **Change master data**.
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.

5

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

   - 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 62

Master data for a container

Enter the following master data for a container.

Table 21: Master Data for a Container

Property	Description
Name	Container name.
Canonical name	Canonical name of the container. The canonical name is generated automatically and should not be changed.
Distinguished	Distinguished name of the container. The distinguished name is

Property	Description
name	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

- Linking user accounts to employees on page 64
- Supported user account types on page 65
- Entering user account master data on page 71

Linking user accounts to employees

The central component of 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, 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 can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account , a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism and subsequent process handling.

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

- When user accounts are inserted, they can be automatically assigned to an existing employee. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this procedure is not the default procedure for One Identity Manager. Define criteria for finding employees for automatic employee assignment.
- Employees and user accounts can be entered manually and assigned to each other.

Related Topics

- Setting up account definitions on page 21
- Entering user account master data on page 71
- Automatic assignment of employees to user accounts on page 77
- 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, service accounts, or privileged user accounts can be mapped in One Identity Manager.

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

- Identity

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

  Table 22: Identities of user accounts

Identity	Description	Value of the IdentityType column
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.	Organizational
Personalized	User account with administrative permissions,	Admin

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

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

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

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

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

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

- Privileged user account

  Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are marked as **Privileged user account** (Column `IsPrivilegedAccount`).

Detailed information about this topic

- Default user accounts on page 67
- Administrative user accounts on page 67
- Providing administrative user accounts for one employee on page 68
- Providing administrative user accounts for several employees on page 69
- Privileged user accounts on page 70

Default user accounts

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

To create default user accounts through account definitions

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

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

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

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

   Specify in the departments, cost centers, locations, or business roles 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.

Related Topics

- Setting up account definitions on page 21

Administrative user accounts

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

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

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

Related Topics

- Providing administrative user accounts for one employee on page 68
- Providing administrative user accounts for several employees on page 69

Providing administrative user accounts for one employee

Prerequisites

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

To prepare an administrative user account for a person

1. Label the user account as a personalized admin identity.
    a.
    b. Select the user account in the result list.
    c. Select **Change master data**.
    d. On the **General** tab, in the **Identity** selection list, select **Personalized administrator identity**.
2. Link the user account to the employee who will be using this administrative user account.
    a.
    b. Select the user account in the result list.
    c. Select **Change master data**.
    d. On the **General** tab, in the **Person** selection list, select the employee who will be using this administrative user account.

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

Related Topics

- Providing administrative user accounts for several employees on page 69
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Providing administrative user accounts for several employees

Prerequisite

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

To prepare an administrative user account for multiple employees

1. Label the user account as a shared identity.
    a.
    b. Select the user account in the result list.
    c. Select **Change master data**.
    d. On the **General** tab, in the **Identity** selection list, select **Shared identity**.
2. Link the user account to a dummy employee.
    a.
    b. Select the user account in the result list.
    c. Select **Change master data**.
    d. On the **General** tab, select the dummy employee from the **Employee** selection list.

    TIP: If you are the target system manager, you can choose to create a new dummy employee.
3. Assign the employees who will use this administrative user account to the user account.
    a.
    b. Select the user account in the result list.
    c. Select the task **Assign employees authorized to use**.
    d. Assign employees in **Add assignments**.

TIP: In the **Remove assignments** area, you can remove the assignment of employees.

To remove an assignment

- Select the employee and double click .

Related Topics

- Providing administrative user accounts for one employee on page 68
- For detailed information about mapping employee identities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Privileged user accounts

Privileged user accounts are used to provide employees with additional privileges. This includes administrative user accounts or service accounts, for example. The user accounts are marked as **Privileged user account** (Column `IsPrivilegedAccount`).

NOTE: The criteria according to which user accounts are automatically identified as privileged are defined as extensions to the view definition (ViewAddOn) in the `TSBVAccountIsPrivDetectRule` table (which is a table of the **Union** type). The evaluation is done in the 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 the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts is created.
3. Specify the effect of temporarily or permanently disabling or deleting, or the security risk of an employee on its user accounts and group memberships for each manage level.
4. Create a formatting rule for IT operating data.

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

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

   - In the mapping rule for the `IsPrivilegedAccount` column, use the default value **1** and enable **Always use default value**.

- You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.
- To prevent privileged user accounts from inheriting the Entitlements of the default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and enable **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.

TIP: If customization requires that the login names of privileged user accounts follow a defined naming convention, create the template according to which the login names are formed.

Related Topics

- Setting up account definitions on page 21

Entering user account master data

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

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

To create a user account

1.
2. Click in the result list toolbar.
3. On the master data form, edit the master data for the user account.
4. Save the changes.

To edit master data for a user account

1.
2. Select the user account in the result list and run **Change master data**.
3. Edit the user account's resource data.
4. Save the changes.

Related Topics

- User account master data on page 72
- Linking user accounts to employees on page 64
- Supported user account types on page 65
- Setting up account definitions on page 21

User account master data

Enter the following data for a user account:

Table 23: 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. For a user account with an identity of type **Organizational identity**, **Personalized administrator identity**, **Sponsored identity**, **Shared identity** or **Service identity**, you can create a new employee. To do this, click next to the input field and enter the required employee master data. Which login data is required depends on the selected identity type.
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	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Target system	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 with the manage level.
Last name	The user's last name. If you have assigned an account definition, the input field is automatically filled with the manage level.

Property	Description
Container	Container in which to create the user account. If you have assigned an account definition, the container is determined from the company IT data for the assigned employee depending on the manage level of the user account. When the container is selected, the defined name for the user is created using a formatting rule.
Login name	Name the user uses to log onto the target system. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Name	User account identifier. The identifier is made up of the user's first and last names.
Canonical name	Canonical name of the user account. The canonical name is generated automatically and should not be changed.
Distinguished name	Distinguished name of the user account. The distinguished name is determined using a template and must not be changed.
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the **QER | CalculateRiskIndex** configuration parameter is enabled. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Account expiry date	The date up to which the user can log into a target system with this user account. If a leaving date is specified for an employee, this date is used as the account expiration date depending on the manage level. Any existing account expiry date is overwritten in this case. NOTE: If the employee's leaving date is deleted at a later point in time, the user account expiration date remains intact.
Last login	Date of last target system login.
Password last changed	Data of last password change.
Password	Password for the user account. Based on the **QER | Person | UseCentralPassword** configuration parameter, the central password of the assigned employee is mapped to the password of the user account. 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 Permitted values are: • **Primary identity**: Employee's default user account. • **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • **Personalized administrator identity**: User account with administrative entitlements, used by one employee. • **Sponsored identity**: User account that is used for training purposes, for example. • **Shared identity**: User account with administrative entitlements, used by several employees. Assign all employees show use the user account. • **Service identity**: Service account.
Privileged user account	Specifies whether this is a privileged user account.
Groups can be inherited	Specifies whether the user account can inherit groups via the employee. If this option is set, the user account inherits groups via 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 whether the user account is locked. If a user account is not required for a period of time, you can temporarily disable the user account by using the option <User account is deactivated>.

Related Topics

- Setting up account definitions on page 21
- Password policies for user accounts on page 39
- Initial password for new user accounts on page 49

- Supported user account types on page 65
- Group inheritance based on categories on page 95
- Disabling user accounts on page 82

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 the user account

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 user account in the result list.
2. Select **Change master data**.
3. On the **General** tab, select the manage level in the **Manage level** menu.
4. 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, such as 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.
2. Select the user account in the result list.
3. Select **Assign groups**.
4. Assign groups in **Add assignments**.

   TIP: you can remove the assignment of groups in the **Remove assignments** area.

   To remove an assignment

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

Related Topics

- Target system types on page 53
- Assigning group to user accounts on page 86

Assigning extended properties

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

To specify extended properties for a user account

1.
2. Select the user account in the result list.
3. Select **Assign extended properties**.

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

   TIP: In the **Remove assignments** area, you can remove the assignment of extended properties.

   To remove an assignment

   - Select the extended property and double click .

5. Save the changes.

For 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 24: 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.

Configuration parameter	Meaning
TargetSys-tem\UNS\PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names are listed in a pipe (|) delimited list that is handled as a regular search 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 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 **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 that the manage level to be used is entered as the default manage level.
- Define the search criteria for employees assigned to the target system.

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

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

NOTE:

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

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

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 user accounts in **linked** status.
   a. In Manager, select **Custom target systems | <target system> | User accounts | Linked but not configured | <target system>**.
   b. Select **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 22
- Assigning an account definition to a custom target system on page 37

- Editing search criteria for automatic employee assignment on page 80

Editing search criteria for automatic employee assignment

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

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

NOTE: 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 **Change master data** to assign employees to administrative user account for the respective user account.

To specify criteria for employee assignment

1. Select **Custom target systems | Basic configuration data | <target system>**.
2. Select the 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 25: Standard search criteria for user accounts

Apply to	Column for employee	Column for user account
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

In **Assignments**, you can create a suggestion list for assignments of employees to user accounts based on the search criteria and make the assignment directly. User accounts are

grouped in different views for this.

Table 26: 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 which you want to assign the suggested employees. Multi-select is possible.
   b. Click **Assign selected.**
   c. Confirm the security prompt with **Yes**.

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

   – OR –

2. Click **No employee assignment**.
   a. Click **Select employee** for the user account to which you want to assign an 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**.

      The employees displayed in the **Employee** column are assigned to the selected user accounts.

To remove assignments

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

       The assigned employees are removed 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 77

Disabling user accounts

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. Accounts with the manage level **Full managed** manage level are disabled depending on the account definition settings. For user accounts with a manage level, configure the required behavior using the template in the `UNSAccountB.AccountDisabledPAGUser.IsDisabled` column.

Scenario:

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

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

- If the configuration parameter is set, the employee's user accounts are disabled 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 disable the user account when the configuration parameter is disabled.

1.

2. Select the user account in the result list.

Scenario:

- User accounts not linked to employees.

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

1.
2. Select the user account in the result list.

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 83
- Creating an account definition on page 22
- Setting up manage levels on page 25

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 assignment of an account definition is removed, the user account that was created from this account definition is.

You can delete a user account that was not created using an account definition through the result list or from the menu bar. After you have confirmed the security alert the user account is marked for deletion in the One Identity Manager. The user account is locked in One Identity Manager and 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 `UNSAccountB` in the Designer.

To delete a user account

1. Select **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 a user account

1. Select **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 82

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. In Manager, select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list and run **Change master data**.
3. On the master data form, edit the master data for the group.
4. Save the changes.

Detailed information about this topic

- Group master data on page 85

Group master data

Enter the following master data for a group.

Table 27: Entering Master Data for a Group

Property	Description
Name	Name of the group.
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.
Display name	The display name is used to display the group in the One Identity Manager tools user interface.

Property	Description
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 input field is only visible if the configuration parameter **QER | CalculateRiskIndex** is activated. 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. Select one or more categories from the menu.
Description	Spare text box for additional explanation.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is no permitted.

Related Topics

- Group inheritance based on categories on page 95
- 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**.

Groups can also be assigned to persons via IT Shop requests. So that groups can be assigned using IT Shop requests, employees are added to a shop as customers. 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 53

Assigning groups to departments, cost centers and locations

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

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

1. In Manager, 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 centers** tab.

   TIP: In the **Remove assignments** area, you can remove the assignment of organizations.

   To remove an assignment

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

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

1. Select **Organizations | Departments** in Manager.

   - OR -

   Select **Organizations | Cost centers** in Manager.

   - OR -

In Manager, select **Organizations | Locations**.

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

   TIP: you can remove the assignment of groups in the **Remove assignments** area.

   To remove an assignment

   - Select the group and double click ✓.

5. Save the changes.

Assigning groups to business roles

Installed modules: 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. In Manager, select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign business roles**.
4. Assign business roles in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of business roles.

   To remove an assignment

   - Select the business role and double click ✓.

5. Save the changes.

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

1. In Manager, select **Business roles | <role class>**.
2. Select the business role in the result list.
3. Select **Assign groups custom target systems**.

4. Assign groups in **Add assignments**.

   TIP: you can remove the assignment of groups in the **Remove assignments** area.

   To remove an assignment

   - Select the group and double click .

5. Save the changes.

Assigning user accounts directly 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, such as 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. In Manager, select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign user accounts**.
4. Assign user accounts in **Add assignments**.

   TIP: In the **Remove assignments** area, you can remove the assignment of user accounts.

   To remove an assignment

   - Select the user account and double click .

5. Save the changes.

Adding 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 user accounts belonging to these employees inherit the group.

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

To assign a group to system roles

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

   TIP: In the **Remove assignments** area, you can remove the assignment of system roles.

   To remove an assignment

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

Adding groups to the IT Shop

When you assign a group to a 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 marked with the **IT Shop** option.
- the group must be assigned a service item.

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

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

To add a group to IT Shop.

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

   - OR -

   In Manager, select **Entitlements | Groups** (role-based login).
2. In the result list, select the group.
3. Select **Add to** IT Shop.
4. In **Add assignments**, assign the group to the IT Shop shelves.
5. Save the changes.

To remove a group from individual shelves of the IT Shop

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

   - OR -

   In Manager, select **Entitlements | Groups** (role-based login).
2. In the result list, select the group.
3. Select **Add to** IT Shop.
4. In **Remove assignments**, remove the group from the IT Shop shelves.
5. Save the changes.

To remove a group from all shelves of the IT Shop

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

   - OR -

   In Manager, select **Entitlements | Groups** (role-based login).
2. In the result list, select the group.
3. Select **Remove from all shelves (IT Shop)**.
4. Confirm the security prompt with **Yes**.
5. Click **OK**.

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

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

Related Topics

- Group master data on page 85

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. In Manager, select the category **Custom target systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign groups**.
4. Assign the groups that are are subordinate to the selected group in **Add assignments**.

   TIP: you can remove the assignment of groups in the **Remove assignments** area.

   To remove an assignment

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

Effectiveness of group memberships

Table 28: Configuration Parameter for Conditional Inheritance

Configuration parameter	Effect when set
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. Changes to the parameter require recompiling the database.

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 (table).

The effectiveness of the assignments is mapped in the UNSAccountBInUNSGroupB and BaseTreeHasUNSGroupB via 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 29: Specifying excluded groups (table UNSGroupBExclusionAADGroupExclusion))

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

Table 30: 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 31: 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 | Structures | 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. In Manager, select the category **Custom target systems | <target system> | Groups**.
2. Select a group in the result list.
3. Select **Exclude groups**.

4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.

   - OR -

   In **Remove assignments**, remove the groups that are not longer mutually exclusive.

5. Save the changes.

Group inheritance based on categories

In One Identity Manager, groups can be selectively inherited by user accounts. For this purpose, the groups and the user accounts are divided into categories. The categories can be freely selected and are specified using a mapping rule. Each category is given a specific position within this mapping rule. 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. In the group table enter your categories for the target system-dependent groups. Each table contains the category positions **Position 1** to **Position 31**.

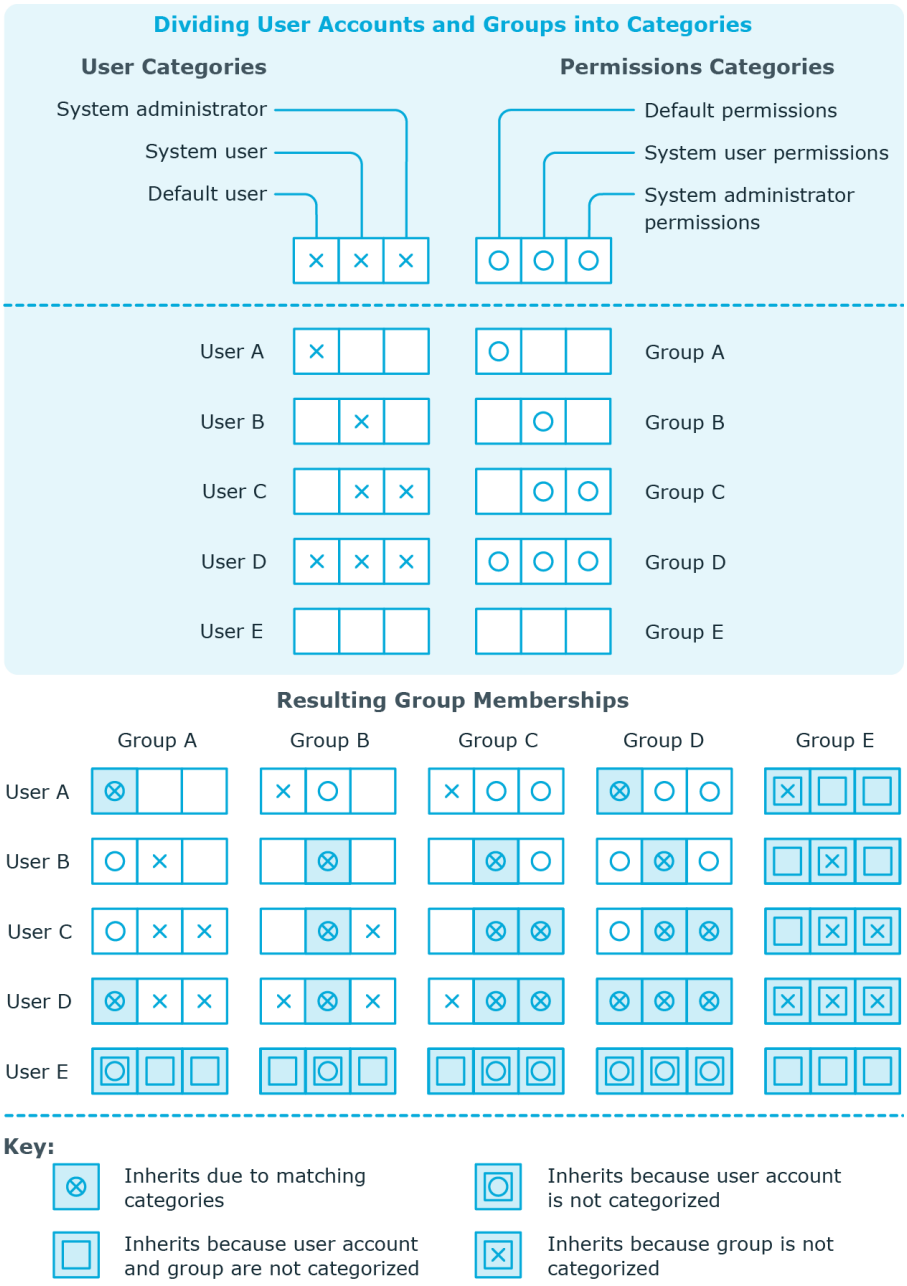
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category item matches an assigned group. The group is also inherited by the user account if the group or the 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 32: 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 60
- User account master data on page 72
- Group master data on page 85

Assigning extended properties

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

To specify extended properties for a group

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

   TIP: In the **Remove assignments** area, you can remove the assignment of extended properties.

   To remove an assignment

   - Select the extended property and double click .
5. Save the changes.

For more detailed information about setting up 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 -

   In the **Remove assignments** view, double click on the permissions controls for which you want to delete the assignment.

5. Save the changes.

Related Topics

- Entering permissions controls on page 99

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 One Identity Manager from the connected target system. You can also add permissions controls in One Identity Manager.

To edit permissions controls

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

   - 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 99

Permissions control master data

Enter the following master data for a permissions control.

Table 33: 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.
Description	Spare text box for additional explanation.

Property	Description
Spare field no. 01 ... Spare field no. 10	Additional company specific information. Use 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 **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 **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**.

   TIP: In the **Remove assignments** area, you can remove the assignment of user accounts.

   To remove an assignment

   - Select the user account and double click .

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 **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**.

   TIP: you can remove the assignment of groups in the **Remove assignments** area.

   To remove an assignment

   - Select the group and double click .

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 34: 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 system 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 103

Overview of all assignments

The **Overview of all assignments** report is displayed for some objects, such as authorizations, compliance rules, or roles. The report finds all the roles, for example, departments, cost centers, locations, business roles and IT Shop structures in which there are 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 or another system entitlement, all roles are determined in which there are employees with this group or system entitlement.
- If the report is created for a compliance rule, all roles are determined in which there are employees 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**.
- Click the **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain employees with the selected base object.

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

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

Table 35: 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.

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 36: 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 provide users with the login data for their user accounts. The **Employee - new user account created** mail template is used.

Configuration parameter	Meaning
TargetSystem\UNS\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword	This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The **Employee - initial password for new user account** mail template is used.
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. The **Employee - new user account with default properties created** mail template is used.
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 are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.*\$`

About us

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

Contacting us

For sales 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

D

E

I

L

M

N

O

P

T

U