One Identity Manager 8.0.1

Administration Guide for Connecting to a Universal Cloud Interface

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 a Universal Cloud Interface
Updated - March 2018
Version - 8.0.1

Contents

1

Managing Universal Cloud Interface Environments

One Identity Manager supports the implementation of Identity and Access Governance demands in IT environments, which are often a mix of traditional, internally hosted applications and modern cloud applications. Users and entitlements from cloud applications can be mapped in One Identity Manager. This makes it possible to also use Identity and Access Governance processes such as attestation, identity audit, management of users and system entitlements, IT Shop or report subscriptions for cloud applications.

Data protection policies, such as the General Data Protection Regulation, require agreement as to which employee data can be stored in cloud applications. If the system environment is configured appropriately, One Identity Manager guarantees that cloud applications and their administrators have no access to any employee master data or Identity and Access Governance processes respectively. For this reason, cloud applications are managed in two separate modules, which can be installed in separate databases if necessary.

The Universal Cloud Interface Module provides the interface through which users and permissions can be transferred from cloud applications to a One Identity Manager database. Synchronization with the cloud applications is configured and executed at this stage. Each cloud application is mapped as its own base object in One Identity Manager. The user data is saved as user accounts, groups and permissions controls and can be organized into containers. They cannot be edited in One Identity Manager. There is no connection made to identities (employees).

Identities are connected in the Cloud Systems Management Module; user accounts, groups and permissions controls can be created and edited. This allows Identity and Access Governance processes to be used for managing cloud user accounts and their permissions. Data is exchanged between the Universal Cloud Interface and Cloud System Management modules by synchronization. Provisioning processes ensure that object changes are transferred from the Cloud Systems Management Module to the Universal Cloud Interface Module.

Automated interfaces for provisioning changes from the Universal Cloud Interface Module to the cloud application can (on technical grounds) or should (due to too few changes) not be applied to certain cloud applications. In this case, changes can be manually provisioned.

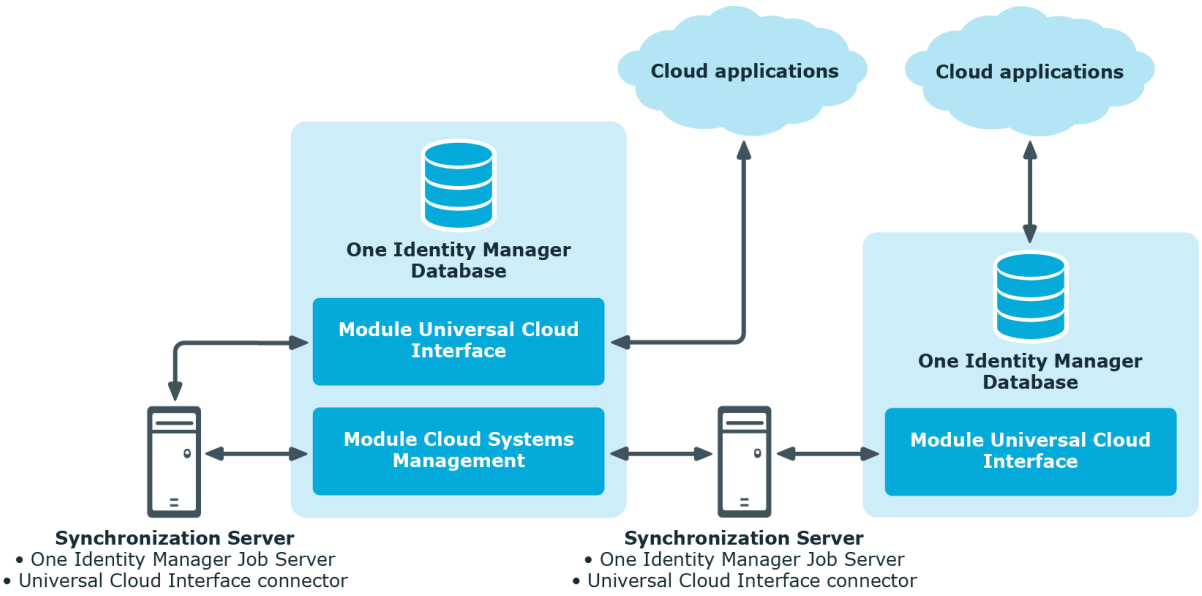
Because only data that must be available in the cloud application is saved in the Universal Cloud Interface Module, the module can be installed in a separate database. This database may be outside the company's infrastructure.

The cloud solution One Identity Connect For Cloud provides a simple and comprehensive solution for integrating cloud applications and for meeting the requirements of hybrid solution scenarios.

Architecture Overview

A synchronization server installed with the Universal Cloud Interface Module connector is required for synchronizing cloud applications in the Universal Cloud Interface. The Universal Cloud Interface Module can be in the same One Identity Manager database in which the Cloud Systems Management Module is installed. Synchronization can also be set up with another One Identity Manager database, which is on an external database server.

Figure 1: Architecture for synchronization



For more detailed information about communicating between the Universal Cloud Interface and cloud application, see the One Identity Manager Administration Guide for Connecting to Cloud Applications.

One Identity Manager Users for Managing Cloud Target Systems

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

Table 1: Users

User	Task
Target system administrators	Target system administrators must be assigned to the application role **Target system | Administrators**. Users with this application role: • Administrate application roles for individual target systems types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles are conflicting for target system managers • Authorize other employee to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the application role **Target systems | Cloud target systems** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare groups for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer, as required. • Create system users and permissions groups for non-role based login to administration tools, as required.

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

2

Setting up Synchronization with a Cloud Application in the Universal Cloud Interface

Data is exchanged between the Universal Cloud Interface and Cloud System Management modules by synchronization. In order to apply Identity and Data Governance processes to cloud application objects, you must set up synchronization between the two modules.

NOTE: The terms "target system" and "(One Identity Manager) database" are used frequently in the following. The term "target system" always means a cloud application in the Universal Cloud Interface. "One Identity Manager database" or "database" refers to the objects in the Cloud Systems Management Module.

Table 2: Terms

	One Identity Manager database	Target System
Connected system	Cloud Systems Management Module	Universal Cloud Interface Module
Base object	Cloud target system	Cloud application

The mapping defines how schema types of the connection systems are mapped to each other. For more information, see Appendix: Default Project Template for Cloud Application in the Universal Cloud Interface on page 127.

To transfer objects from a cloud application into the Cloud Systems Management Module for the first time

1. Provide One Identity Manager users with the required permissions for setting up synchronization and post-processing of synchronization objects.
2. The One Identity Manager components for managing cloud target systems are available if the configuration parameter "TargetSystem\CSM" 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.

3. Install and configure a synchronization server and declare the server as Job server in One Identity Manager.
4. Create a synchronization project with the Synchronization Editor.

   The cloud application must already be available in the Universal Cloud Interface Module.

Detailed information about this topic

- Users and Permissions for Synchronizing on page 12
- Setting Up the Synchronization Server on page 13
- Creating a Synchronization Project for Initial Synchronization of a Cloud Application on page 16

For more detailed information about setting up initial synchronization with a cloud application, see the One Identity Manager Administration Guide for Connecting to Cloud Applications.

Users and Permissions for Synchronizing

The following users are involved in synchronizing One Identity Manager with a cloud application in the Universal Cloud Interface.

Table 3: Users for Synchronization

User	Permissions
Users for accessing the Cloud Application in the Universal Cloud Interface	To log on to the database containing the Universal Cloud Interface, use: • Role-based login: a user with the application role **Universal Cloud Interface | Administrators** - OR - • Non role-based login: a system user with the permissions group "DPR_EditRights_Methods".
One Identity Manager Service user account	The user account for the One Identity Manager Service requires access rights to carry out operations at file level (issuing user rights, adding directories and files to be edited). The user account must belong to the group "Domain Users".

User	Permissions
	The user account must have the extended access right "Log on as a service". The user account requires access rights to the internal web service. NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager. In the default installation the One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems)
User for accessing the One Identity Manager database	The default system user "Synchronization" is available to run synchronization over an application server.

Setting Up the Synchronization Server

A server with the following software must be available for setting up synchronization:

- One Identity Manager Service
  - Install One Identity Manager components with the installation wizard.
    1. Select the option **Select installation modules with existing database**.
    2. Select the machine role **Server | Job server**.

  For more detailed information about system requirements for installing the One Identity Manager Service, see the One Identity Manager Installation Guide.

The synchronization server must be declared as a Job server in One Identity Manager.

Use the Server Installer to install the One Identity Manager Service. This program executes the following steps.

- Setting up a Job server.
- Specifying machine roles and server function for the Job server.
- Remote installation of One Identity Manager Service components corresponding to the machine roles.
- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

NOTE: The program executes remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program. Remote installation is only supported within a domain or a trusted domain.

To install and configure the One Identity Manager Service remotely on a server

1. Start the program Server Installer on your administrative workstation.
2. Enter valid data for connecting to One Identity Manager on the **Database connection** page and click **Next**.
3. Specify on which server you want to install the One Identity Manager Service on the **Server properties** page.
   a. Select a job server in the **Server** menu.

      - OR -

      Click **Add** to add a new job server.

   b. Enter the following data for the Job server.

      Table 4: Job Servers Properties

Property	Description
Server	Name of the Job servers.
Queue	Name of 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.
Full server name	Full name of the server in DNS syntax. Example: `<name of server>.<fully qualified domain name>`

      NOTE: Use the **Advanced** option to edit other Job server properties. You can use the Designer to change properties at a later date.
4. Specify which job server roles to include in One Identity Manager on the **Machine role** page. Installation packages to be installed on the Job server are found depending on the selected machine role.
   - Job Server

5. Specify the server's functions in One Identity Manager on the **Server functions** page. One Identity Manager processes are handled depending on the server function.

   The server's functions depend on which machine roles you have selected. You can limit the server's functionality further here.

   - Universal Cloud Interface connector

6. Check the One Identity Manager Service configuration on the **Service settings** page.

   NOTE: The initial service configuration is already predefined. If further changes need to be made to the configuration, you can do this later with the Designer. For more detailed information about configuring the service, see One Identity Manager Configuration Guide.

7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on the **Select installation source** page.
10. Select the file with the private key on the page **Select private key file**.

    NOTE: This page is only displayed when the database is encrypted.

11. Enter the service's installation data on the **Service access** page.

Table 5: Installation Data

Data	Description
Computer	Server on which to install and start the service from. ***To select a server*** • Enter the server name. - OR - • Select a entry from the list.
Service account	One Identity Manager Service user account data. ***To enter a user account for the One Identity Manager Service*** • Set the option **Local system account**. This starts the One Identity Manager Service under the account "NT AUTHORITY\SYSTEM". - OR - • Enter user account, password and password confirmation. The One Identity Manager Service farm's server farm account must be used as user account for SharePoint.

Data	Description
Installation account	Data for the administrative user account to install the service. ***To enter an administrative user account for installation*** **Enable** Advanced • . • Enable the option **Current user**. This uses the user account of the current user. - OR - • Enter user account, password and password confirmation.

12. Click **Next** to start installing the service.

    Installation of the service occurs automatically and may take some time.

13. Click **Finish** on the last page of the Server Installer.

    NOTE: The is entered with the name "One Identity Manager Service" in the server's service administration.

Creating a Synchronization Project for Initial Synchronization of a Cloud Application

Use the Synchronization Editor to set up synchronization between the Cloud Systems Management Module and the Universal Cloud Interface Module. The following describes the steps for initial configuration of a synchronization project.

After the initial configuration, you can customize and configure workflows within the synchronization project. Use the workflow wizard in the Synchronization Editor for this. The Synchronization Editor also provides different configuration options for a synchronization project.

Have the following information available for setting up a synchronization project.

Table 6: Information Required for Setting up a Synchronization Project

Data	Explanation
Cloud application	Name of the cloud application in the Universal Cloud Interface Module to synchronize.
Synchronization server	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries

Data	Explanation
	required for synchronization and administration with the One Identity Manager database, are processed by the synchronization server. The One Identity Manager Service with the Universal Cloud Interface connector must be installed on the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server. **Table 7: Additional Properties for the Job Server** **Property** / **Value** Server Function: Universal Cloud Interface connector Machine role: Server/Job server For more information, see Setting Up the Synchronization Server on page 13.
One Identity Manager Database Connection Data	SQL Server: • Database server • Database • Database user and password • Specifies whether Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication. Oracle: • Species whether access is direct or through the Oracle client Which connection data is required, depends on how this option is set. • Database server • Oracle instance port • Service name • Oracle database user and password • Data source (TNS alias name from `TNSNames.ora`)
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with target system to do this.

Data	Explanation
	Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access to the workstation is not possible, you can set up a remote connection. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • `RemoteConnectPlugin` is installed • Universal Cloud Interface connector is installed The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required. For more detailed information about setting up a remote connection, see the One Identity Manager Target System Synchronization Reference Guide.

NOTE: The following sequence describes how you configure a synchronization project if the Synchronization Editor is both:

- In default mode
- Started from the launchpad

Additional settings can be made if the project wizard is run in expert mode or is started directly from the Synchronization Editor. Follow the project wizard instructions through these steps.

To set up initial synchronization project for a cloud application

1. Start the Launchpad and log on to the One Identity Manager database.

   NOTE: If synchronization is executed by an application server, connect the database through the application server.

2. Select the entry **Universal Cloud Interface target system type**. Click **Run**.

   This starts the Synchronization Editor's project wizard.

3. Specify how the One Identity Manager can access the target system on the **System access** page.
   - If you have access from the workstation from which you started the Synchronization Editor, do not set anything.
   - If you do not have access from the workstation from which you started the Synchronization Editor, you can set up a remote connection.

In this case, set the option **Connect using remote connection server** and select, under **Job server**, the server you want to use for the connection.

4. Click **Next** on the start page of system connection wizard.
5. Select the database system to which you want to connect on the **Select database system** page.
6. Enter the connection data for the database containing the Universal Cloud Interface Module on the **Connection parameter** page.

Table 8: SQL Server Database Connection Data

Data	Description
Server	Database server.
Windows authentication	Specifies whether Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
User	Database user.
Password	Database user password.
Database	Database.

Table 9: Oracle Database Connection Data

Data	Description
Direct access (without Oracle client)	Set this option for direct access. Deactivate this option for access via Oracle Clients. Which connection data is required, depends on how this option is set.
Server	Database server.
Port	Oracle instance port.
Service name	Service name.
User	Oracle database user.
Password	Database user password.
Data source	TNS alias name from `TNSNames.ora`.

- To enter additional information about the database connection, click **Advanced options**.
- To test whether you can reach the database, click **Test**.

7. Enter the private key for encrypting the database on the **Encryption** page.

8. You can save the connection data on the last page of the system connection wizard.
    - Set the option **Save connection locally** to save the connection data. This can be reused when you set up other synchronization projects.
    - Click **Finish**, to end the system connection wizard and return to the project wizard.
9. Verify the One Identity Manager database connection data on the **One Identity Manager connection** page. The data is loaded from the connected database. Reenter the password.

    NOTE: Reenter all the connection data if you are not working with an encrypted One Identity Manager database and no synchronization project has been saved yet in the database. This page is not shown if a synchronization project already exists.
10. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.
11. Select the cloud application to synchronize on the **Select cloud application** page.
12. Specify how system access should work on the page **Restrict target system access**. You have the following options:

Table 10: Specifying Target System Access

Option	Meaning
Read-only access to target system.	Specifies whether a synchronization workflow should be set up to initially load the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of "One Identity Manager". • Processing methods in the synchronization steps are only defined in synchronization direction "One Identity Manager".
Changes are also made to the target system.	Specifies whether a provisioning workflow should be set up in addition to the synchronization workflow to initially load the target system. The provisioning workflow displays the following characteristics: • Synchronization in the direction of the "target system" • Processing methods are only defined in the synchronization steps in synchronization direction "target system".

Option	Meaning
	• Synchronization steps are only created for such schema classes whose schema types have write access.

13. Select the synchronization server to execute synchronization on the **Synchronization server** page.

    If the synchronization server is not declare as a job server in the One Identity Manager database yet, you can add a new job server.

    - Click to add a new job server.
    - Enter a name for the job server and the full server name conforming to DNS syntax.
    - Click **OK**.

      The synchronization server is declared as job server for the target system in the One Identity Manager database.

      NOTE: Ensure that this server is set up as the synchronization server after saving the synchronization project.

14. Click **Finish** to complete the project wizard.

    Two start up configurations and two default schedules are created for regular synchronization.

    Table 11: Start up Configurations

Start up configuration	Execution Interval
Synchronization of the cloud application	Daily
Synchronization of pending changes	Hourly

    The synchronization project is created, saved and enabled immediately.

    NOTE: If the synchronization project is not going to be executed immediately, disable the option **Activate and save the new synchronization project automatically**.

    In this case, save the synchronization project manually before closing the Synchronization Editor.

    NOTE: The target system connection data is saved in a variable set, which you can change in the Synchronization Editor under **Configuration | Variables** if necessary.

To configure the content of the synchronization log

1. To configure the synchronization log for target system connection, select the category **Configuration | Target system**.

2. To configure the synchronization log for the database connection, select the category **Configuration | One Identity Manager connection**.
3. Select **General** view and click **Configure...**.
4. Select the **Synchronization log** view and set **Create synchronization log**.
5. Enable the data to be logged.

   NOTE: Certain content create a lot of log data.

   The synchronization log should only contain the data necessary for error analysis and other evaluations.

6. Click **OK**.

To synchronize on a regular basis

1. Select the category **Configuration | Start up configurations**.
2. Select a start up configuration in the document view and click **Edit schedule...**.
3. Edit the schedule properties.
4. To enable the schedule, click **Activate**.
5. Click **OK**.

To start initial synchronization manually

1. Select the category **Configuration | Start up configurations**.
2. Select a start up configuration in the document view and click **Execute**.
3. Confirm the security prompt with **Yes**.

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

To select user accounts through account definitions

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

Detailed information about this topic

- One Identity Manager Target System Synchronization Reference Guide

Related Topics

- Setting Up the Synchronization Server on page 13
- Users and Permissions for Synchronizing on page 12
- Start Up Configuration on page 23
- Show Synchronization Results on page 24
- Customizing Synchronization Configuration on page 25
- Speeding Up Synchronization with Revision Filtering on page 28
- Appendix: Default Project Template for Cloud Application in the Universal Cloud Interface on page 127
- Setting Up Account Definitions on page 34
- Automatic Assignment of Employees to User Accounts on page 91

Start Up Configuration

The project wizard adds two start up configurations that run cloud application synchronization.

- Synchronization of the cloud application

  This synchronizes cloud application objects such as user accounts, groups, group memberships. The workflow "Initial synchronization" is used. Synchronization is run on a daily basis with the default schedule.

- Synchronization of pending changes

  If cloud objects in the Cloud Systems Management Module are changed, the changes must first be transfered to the Universal Cloud Interface Module and then they can be provisioned in the cloud application itself. To track whether the changes have been successfully provisioned in the cloud application, they are labeled with "Pending changes". The details, time of creation and processing status of every pending change are saved. Once provisioning is complete, the processing status must be transferred from the Universal Cloud Interface to the Cloud Systems Management Module. To do this, run the start up configuration "Synchronization of pending changes". This uses the workflow "Initial synchronization". Synchronization is run on an hourly basis with the default schedule.

Related Topics

- Provisioning Object Changes on page 118

Show Synchronization Results

Synchronization results are summarized in the synchronization log. You can specify the extent of the synchronization log for each system connection individually. One Identity Manager provides several reports in which the synchronization results are organized under different criteria.

To display a synchronization log

1. Select the category **Logs**.
2. Click ▶ in the navigation view toolbar.

   Logs for all completed synchronization runs are displayed in the navigation view.
3. Select a log by double-clicking on it.

   An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log.

1. Select the category **Logs**.
2. Click ⚡ in the navigation view toolbar.

   Logs for all completed provisioning processes are displayed in the navigation view.
3. Select a log by double-clicking on it.

   An analysis of the provisioning is show as a report. You can save the report.

The log is marked in color in the navigation view. This mark shows you the execution status of the synchronization/provisioning.

Synchronization logs are stored for a fixed length of time. The retention period is set in the configuration parameter "DPR\Journal\LifeTime" and its sub parameters.

To modify the retention period for synchronization logs

- Set the configuration parameter "Common\Journal\LifeTime" in the Designer and enter the maximum retention time for entries in the database journal. Use the configuration sub parameters to specify the retention period for each warning level.
- If there is a large amount of data, you can specify the number of objects to delete per DBQueue Processor operation and run in order to improve performance. Use the configuration parameters "Common\Journal\Delete\BulkCount" and "Common\Journal\Delete\TotalCount" to do this.
- Configure and set the schedule "Delete journal" in the Designer.

Customizing Synchronization Configuration

You have used the Synchronization Editor to set up a synchronization project for initial synchronization with Universal Cloud Interface. You can use this synchronization project to load cloud application objects into the Cloud Systems Management Module. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the Universal Cloud Interface environment.

You must customize the synchronization configuration in order to regularly compare the cloud application and to synchronize changes.

- To use the Cloud Systems Management Module as master system during synchronization, create a workflow with synchronization in the direction of the "Target system".
- To specify which target system objects and database object are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- You can use variables to create generally applicable synchronization configurations which contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes or processing methods, for example.
- Use variables to set up a synchronization project which can be used for several different cloud applications. Store the connection parameter as a variable for logging in to the databases.
- Update the schema in the synchronization project, if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

IMPORTANT: As long as synchronization is running, you must not start another synchronization for the same target system. This applies especially, if the same synchronization objects would be processed.

- The moment another synchronization is started with the same start up configuration, the running synchronization process is stopped and given the status, "Frozen". An error message is written to the One Identity Manager Service log file.
- If another synchronization is started with another start up configuration, that addresses same target system, it may lead to synchronization error or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration. Group start up configurations with the same start up behavior.

For more detailed information about configuring synchronization, see the One Identity Manager Target System Synchronization Reference Guide.

Detailed information about this topic

- How to Configure Universal Cloud Interface Synchronization on page 26
- Configuring Synchronization of Different Cloud Applications on page 26
- Updating Schemas on page 27

How to Configure Universal Cloud Interface Synchronization

The synchronization project for initial synchronization provides a workflow for initial loading of target system objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). You also require a workflow with synchronization in the direction of the "target system" to use One Identity Manager as the master system for synchronization.

To create a synchronization configuration for synchronizing Universal Cloud Interface

1. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the target system. Create new maps if required.
3. Create a new workflow with the workflow wizard.

   This adds a workflow for synchronizing in the direction of the target system.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Related Topics

- Configuring Synchronization of Different Cloud Applications on page 26

Configuring Synchronization of Different Cloud Applications

Prerequisites

- All virtual schema properties used in the mapping must exist in the extended schema of both cloud applications.

To customize a synchronization project for synchronizing another cloud application

1. Open the synchronization project in the Synchronization Editor.
2. Create a new base object for the other cloud application. Use the wizards to attach a base object.
    - Select the Universal Cloud Interface connector in the wizard and enter the connection parameters. The connection parameters are saved in a special variable set.

      A start up configuration is created, which uses the new variable set.
3. Change other elements of the synchronization configuration as required.
4. Save the changes.
5. Run a consistency check.

Related Topics

- How to Configure Universal Cloud Interface Synchronization on page 26

Updating Schemas

All the schema data (schema types and schema properties) of the target system schema and the One Identity Manager schema are available when you are editing a synchronization project. Only a part of this data is really needed for configuring synchronization. If a synchronization project is finished, the schema is compressed to remove unnecessary data from the synchronization project. This can speed up loading the synchronization project. Deleted schema data can be added to the synchronization configuration again at a later point.

If the target system schema or the One Identity Manager schema has changed, these changes must also be added to the synchronization configuration. Then the changes can be added to the schema property mapping.

To include schema data that have been deleted through compressing and schema modifications in the synchronization project, update each schema in the synchronization project. This may be necessary if:

- A schema was changed by:
    - Changes to a target system schema
    - Customizations to the One Identity Manager schema
    - A One Identity Manager update migration
- A schema in the synchronization project was shrunk by:
    - Activating the synchronization project
    - Synchronization project initial save
    - Compressing a schema

To update a system connection schema

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Target system**.

   - OR -
   Select the category

   Configuration | One Identity Manager connection.
3. Select the view **General** and click **Update schema**.
4. Confirm the security prompt with **Yes**.

   This reloads the schema data.

To edit a mapping

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Mappings**.
3. Select a mapping in the navigation view.

   Opens the Mapping Editor. For more detailed information about editing mappings, see One Identity Manager Target System Synchronization Reference Guide.

NOTE: The synchronization is deactivated if the schema of an activated synchronization project is updated. Reactivate the synchronization project to synchronize.

Speeding Up Synchronization with Revision Filtering

When you start synchronization, all synchronization objects are loaded. Some of these objects have not be modified since the last synchronization and, therefore, must not be processed. Synchronization is accelerated by only loading those object pairs that have changed since the last synchronization. One Identity Manager uses revision filtering to accelerate synchronization.

One Identity Manager supports revision filtering. The date of the last target system object change (column `XDateUpdated`) is used as revision counter. Each synchronization save its last execution date as revision in the the One Identity Manager database (table `DPRRevisionStore`, column `Value`). This value is used as a comparison for revision filtering when the same workflow is synchronized the next time. When this workflow is synchronized the next time, the target system objects' change date is compared with the revision saved in the One Identity Manager database. Only those objects that have been changed since this date are loaded from the target system.

The revision is found at start of synchronization. Objects changed after this point are included with the next synchronization.

Revision filtering can be applied to workflows and start up configuration.

To permit revision filtering on a workflow

- Open the synchronization project in the Synchronization Editor.
- Edit the workflow properties. Select the entry **Use revision filter** from **Revision filtering**.

To permit revision filtering for a start up configuration

- Open the synchronization project in the Synchronization Editor.
- Edit the start up configuration properties. Select the entry **Use revision filter** from **Revision filtering**.

For more detailed information about revision filtering, see the One Identity Manager Target System Synchronization Reference Guide.

Post-Processing Outstanding Objects

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

Objects marked as outstanding:

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

Start target system synchronization to do this.

To post-process outstanding objects

1. Select the category **Cloud target systems | Target system configuration: Universal Cloud Interface**.

   All tables assigned to the target system type Universal Cloud Interface as synchronization tables are displayed in the navigation view.
2. Select the table whose outstanding objects you want to edit in the navigation view.

   This opens the target system synchronization form. All objects are shown here that are marked as outstanding.

   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 12: Methods for handling outstanding objects

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

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

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

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

To disable bulk processing

- Deactivate in the form toolbar.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the option **Connection is read only** must no be set for the target system connection.

The target system type determines, which tables are going to be synchronized. You cannot synchronize custom table in the Cloud Systems Management Module. This means you cannot configure target system configuration for custom tables.

To display the target system synchronization configuration

1. Select the category **Cloud Target Systems | Basic configuration data | Target system types**.

2. Select the target system type Universal Cloud Interface in the result list.
3. Select **Assign synchronization tables** in the task view.

   All the tables that could be synchronized are enabled.
4. Select **Configure tables for publishing**.

   The option **Can be published** is set for all table with outstanding objects in the target system.

Help for Analyzing Synchronization Issues

You can generate a report for analyzing problems which occur during synchronization, for example, insufficient performance. The report contains information such as:

- Consistency check results
- Revision filter settings
- Scope applied
- Analysis of the synchronization buffer
- Object access times in the One Identity Manager database and in the target system

To generate a synchronization analysis report

1. Open the synchronization project in the Synchronization Editor.
2. Select the menu **Help | Generate synchronization analysis report** and answer the security prompt with **Yes**.

   The report may take a few minutes to generate. It is displayed in a separate window.
3. Print the report or save it in one of the available output formats.

Deactivating Synchronization

Regular synchronization cannot be started until the synchronization project and the schedule are active.

To prevent regular synchronization

- Select the start up configuration and deactivate the configured schedule.

  Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited extend. The schema in the synchronization project must be updated if schema modifications are required. The synchronization project is deactivated in this case and can be edited again.

Furthermore, the synchronization project must be deactivated if synchronization should not be started by any means (not even manually).

To deactivate the loaded synchronization project

1. Select **General** on the start page.
2. Click **Deactivate project**.

Detailed information about this topic

- Creating a Synchronization Project for Initial Synchronization of a Cloud Application on page 16

3

Base Data for Managing Universal Cloud Interface

The following data is relevant for managing cloud application in the Cloud Systems Management Module.

- Configuration parameter

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

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

  For more information, see Appendix: Configuration Parameters for Managing Cloud Target Systems on page 124.

- Target system types

  Target system types are required for configuring target system comparisons. Tables containing outstanding objects are maintained on target system types.

  For more information, see Post-Processing Outstanding Objects on page 29.

- Account definitions

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

  For more information, see Setting Up Account Definitions on page 34.

- Password policies

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

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

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

For more information, see Password Policies on page 52.

- 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 60.

- 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 62.

- Target system managers

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

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

  For more information, see Target System Managers on page 64.

- Servers

  Servers must recognize your server's functionality in order to handle target system specific processes in One Identity Manager. For example, the synchronization server.

  For more information, see Editing a Server on page 66.

Setting Up Account Definitions

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

The data for the user accounts in the respective target system comes from the basic employee data. The assignment of the IT operating data to the employee’s user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role (template processing). Processing is done through

templates. There are predefined templates for determining the data required for user accounts included in the default installation. You can customize templates as required.

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

The following steps are required to implement an account definition:

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

Creating an Account Definition

To create a new account definition

1. Select the category **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list. Select **Change master data** in the task view.

   - OR -

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

Detailed information about this topic

- Master Data for an Account Definition on page 35

Master Data for an Account Definition

Enter the following data for an account definition:

Table 13: Master Data for an Account Definition

Property	Description
Account definition	Account definition name.

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

Property	Description
Retain account definition if permanently disabled	Specifies the account definition assignment to permanently disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition if temporarily disabled	Specifies the account definition assignment to temporarily disabled employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition on deferred deletion	Specifies the account definition assignment on deferred deletion of employees. Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Retain account definition on security risk	Specifies the account definition assignment to employees posing a security risk . Option set: the account definition assignment remains in effect. The user account stays the same. Option not set: the account definition assignment is not in effect.The associated user account is deleted.
Resource type	Resource type for grouping account definitions.
Spare field 01 - spare field 10	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Setting Up Manage Levels

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

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

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

- Unmanaged

  User accounts with a manage level of "Unmanaged" become linked to an employee but do not inherit any other properties. When a new user account is added with this manage level and an employee is assigned, some of the employee's properties are transferred initially. If the employee properties are changed at a later date, the changes are not passed onto the user account.

- Full managed

  User accounts with a manage level of "Full managed" inherit specific properties from the assigned employee.

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

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

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

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

To assign manage levels to an account definition

1. Select the category **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions**.
2. Select an account definition in the result list.
3. Select **Assign manage level** in the task view.
4. Assign manage levels in **Add assignments**.

   - OR -

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

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

To edit a manage level

1. Select the category **Cloud 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 39

Master Data for a Manage Level

Enter the following data for a manage level.

Table 14: Master Data for a Manage Level

Property	Description
Manage level	Name of the manage level.
Description	Spare text box for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: Never: Data is not updated always: Data is always updated Only initially: Data is only initially determined.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily disabled employees retain their group memberships.
Lock user accounts if temporarily disabled	Specifies whether user accounts of temporarily disabled employees are locked.
Retain groups if permanently disabled	Specifies whether user accounts of permanently disabled employees retain group memberships.
Lock user accounts if permanently disabled	Specifies whether user accounts of permanently disabled employees are locked.
Retain groups on deferred deletion	Specifies whether user accounts of employees marked for deletion retain their group memberships.

Property	Description
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.

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

To create a mapping rule for IT operating data

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

Table 15: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set.
Source	Specifies which roles to use in order to find the user account properties. You have the following options: • Primary department • Primary location

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

4. Save the changes.

Related Topics

- Determining IT Operating Data on page 41

Determining IT Operating Data

In order for an employee to create user accounts with the manage level "Full managed", the necessary IT operating data must be determined. The operating data required to automatically supply an employee with IT resources is shown in the departments, locations, cost centers, and business roles. An employee is assigned to one primary location, one primary department, one primary cost center or one primary business role. The necessary IT operating data is ascertained from these assignments and used in creating the user accounts. Default values are used if valid IT operating data cannot be found over the primary roles.

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

Example:

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

Create an account definition A for the default user account of the cloud target system A and an account definition B for the administrative user account of cloud target system 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 cloud target system A. This IT operating data is used for standard user accounts. In addition, specify the effective account definition B IT operating data for department A. This IT operating data is used for administrative user accounts.

To specify IT operating data

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

Table 16: IT Operating Data

Property	Description
Organization/Business role	Department, cost center, location or business role for which the IT operating data is valid.
Effects on	IT operating data application scope. The IT operating data can be used for a target system or a defined account definition. ***To specify an application scope*** a. Click → next to the text box. b. Select the table under **Table**, which maps the target system or the table `TSBAccountDef` for an account definition. c. Select the concrete target system or concrete account definition under **Effects on**. d. Click **OK**.
Column	User account property for which the value is set. Columns using the script template `TSB_ITDataFromOrg` in their template are listed. For more detailed information, see the One Identity Manager Target System Base Module Administration Guide.
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 40

Modifying IT Operating Data

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

Prerequisites

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

  - OR -

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

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

To execute the template

1. Select the category **Cloud 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 applied to the object property after modifying the IT operating data.
Selection	Specifies whether the modification is applied to the user account.

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

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

Assigning Account Definitions to Employees

Account definitions are assigned to company employees. Indirect assignment is the default method for assigning account definitions to employees. Account definitions are assigned to departments, cost centers, locations or roles. The employees are categorized into these departments, cost centers, locations or roles depending on their function in the company and thus obtain their account definitions. To react quickly to special requests, you can assign individual account definitions directly to employees. You can automatically assign special account definitions to all company employees. It is possible to assign account definitions to the IT Shop as requestable products. A department manager can then request user accounts from the Web Portal for his staff. It is also possible to add account definitions to system roles. These system roles can be assigned to employees through hierarchical roles or directly or added as products in the IT Shop.

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

NOTE: If a user account already exists and is disabled, then it is re-enabled. You have to alter the user account manage level afterwards in this case.

Prerequisites for indirect assignment of account definitions to employees

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

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

Detailed information about this topic

Assigning Account Definitions to Departments, Cost Centers and Locations

To add account definitions to hierarchical roles

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Business Roles on page 45
- Assigning Account Definitions to all Employees on page 46
- Assigning Account Definitions Directly to Employees on page 47
- Assigning Account Definitions to System Roles on page 47
- Adding Account Definitions in the IT Shop on page 48

Assigning Account Definitions to Business Roles

Installed Modules: Business Roles Module

To add account definitions to hierarchical roles

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 45
- Assigning Account Definitions to all Employees on page 46
- Assigning Account Definitions Directly to Employees on page 47
- Assigning Account Definitions to System Roles on page 47
- Adding Account Definitions in the IT Shop on page 48

Assigning Account Definitions to all Employees

To assign an account definition to all employees

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

   IMPORTANT: Only set this option if you can ensure that all current internal employees in the database and all pending newly added internal employees obtain a user account in this target system.
5. Save the changes.

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

NOTE: Disable the option **Automatic assignment to employees** to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing assignments remain intact.

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 45
- Assigning Account Definitions to Business Roles on page 45
- Assigning Account Definitions Directly to Employees on page 47
- Assigning Account Definitions to System Roles on page 47
- Adding Account Definitions in the IT Shop on page 48

Assigning Account Definitions Directly to Employees

To assign an account definition directly to employees

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 45
- Assigning Account Definitions to Business Roles on page 45
- Assigning Account Definitions to all Employees on page 46
- Assigning Account Definitions to System Roles on page 47
- Adding Account Definitions in the IT Shop on page 48

Assigning Account Definitions to System Roles

Installed Modules: System Roles Module

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

To add account definitions to a system role

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

   - OR -

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

Related Topics

- Assigning Account Definitions to Departments, Cost Centers and Locations on page 45
- Assigning Account Definitions to Business Roles on page 45
- Assigning Account Definitions to all Employees on page 46
- Assigning Account Definitions Directly to Employees on page 47
- Adding Account Definitions in the IT Shop on page 48

Adding Account Definitions in the IT Shop

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

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

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

To add an account definition to the IT Shop

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

   - OR -

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

To remove an account definition from individual IT Shop shelves

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

   - OR -

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

4. Remove the account definition from the IT Shop shelves in **Remove assignments**.
5. Save the changes.

To remove an account definition from all IT Shop shelves

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

   - OR -

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

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

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

Related Topics

- Master Data for an Account Definition on page 35
- Assigning Account Definitions to Departments, Cost Centers and Locations on page 45
- Assigning Account Definitions to Business Roles on page 45
- Assigning Account Definitions Directly to Employees on page 47
- Assigning Account Definitions to System Roles on page 47

Assigning Account Definitions to a Cloud Target System

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

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

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

To assign the account definition to a target system

1. Select the target system in the category **Cloud Target Systems**.
2. Select **Change master data** in the task view.
3. Select the account definition for user accounts from **Account definition (initial)**.
4. Save the changes.

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

Detailed information about this topic

- Automatic Assignment of Employees to User Accounts on page 91

Deleting an Account Definition

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

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

To delete an account definition

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

a. Select the category **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Select **Assign organizations**.

d. Remove the account definition's assignments to departments, cost centers and locations in **Remove assignments**.

e. Save the changes.

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

a. Select the category **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

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

Remove business roles from **Remove assignments**.

d. Save the changes.

5. If the account definition was requested through the IT Shop, it must be canceled and removed from all IT Shop shelves. For more detailed information, see the One Identity Manager IT Shop Administration Guide.

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

a. Select the category **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Select **Change master data** in the task view.

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

e. Save the changes.

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

a. Select the target system in the category **Cloud Target Systems**.

b. Select **Change master data** in the task view.

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

d. Save the changes.

8. Delete the account definition.

a. Select the category **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions**.

b. Select an account definition in the result list.

c. Click , to delete the account definition.

Password Policies

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

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

Detailed information about this topic

Predefined Password Policies

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

Password for logging into One Identity Manager

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

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

Password policy for forming employees' central passwords

An employee's central password is formed from the target system specific user accounts by respective configuration. The password policy "Employee central password policy" defines the settings for the central password (`Person.CentralPassword`).

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

Password policies for target systems

A predefined password policy that you can apply to the user account password columns, is provided for every target system.

NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 8.0.1, the configuration parameter settings for forming passwords are passed on to the target system specific password policies.

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

The password policy "Cloud system password policy" is predefined for cloud target systems. You can apply this password policy to cloud target system user account passwords (`CSMUser.Password`) or to a container.

If the cloud target systems' or containers' password requirements differ, it is recommended that you set up your own password policies for each cloud target system or container.

Editing Password Policies

To edit a password policy

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

   - OR -

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

Detailed information about this topic

- General Master Data for a Password Policy on page 53
- Policy Settings on page 54
- Character Sets for Passwords on page 55
- Custom Scripts for Password Requirements on page 56

General Master Data for a Password Policy

Enter the following master data for a password policy.

Table 17: Master Data for a Password Policy

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

Policy Settings

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

Table 18: Policy Settings

Property	Meaning
Initial password	Initial password for new user accounts. If no password is given when the user account is added or a random password is generated, the initial password is used.
Password confirmation	Reconfirm password.
Min. Length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have.
Max. errors	Maximum number of errors. Set the number of invalid passwords. If the user has reached this number the user account is blocked.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
Password history	Enter the number of passwords to be saved. If the value '5' is entered, for example, the last 5 passwords of the user are

Property	Meaning
	saved.
Min. password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The password strength is not tested if the value is '0'. The values '1', '2', '3' and '4' gauge the required complexity of the password. The value '1' demands the least complex password. The value '4' demands the highest complexity.
Name properties denied	Specifies whether name properties are permitted in the password.

Character Sets for Passwords

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

Table 19: Character Classes for Passwords

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

Custom Scripts for Password Requirements

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

Detailed information about this topic

- Script for Checking a Password on page 56
- Script for Generating a Password on page 57

Script for Checking a Password

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

Syntax for Check Scripts

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

With parameters:

policy = password policy object

spwd = password to test

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

Example for a script for testing a password

A password cannot have '?' or '!' at the beginning. The script checks a given password for validity.

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

```
                Throw New Exception(#LD("Invalid character sequence in password")#)
            End If
        End If
End Sub
```

To use a custom script for checking a password

1. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select the category **Cloud Target Systems | Basic configuration data | Password policies** in the Manager.
    b. Enter the name of the script to test the password in **Check script** on the **Scripts** tab.
    c. Save the changes.

Related Topics

- Script for Generating a Password on page 57

Script for Generating a Password

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

Syntax for Generating Script

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

With parameters:

policy = password policy object

spwd = generated password

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

Example for a script to generate a password

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

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

```
            If pwd(0)="?" Or pwd(0)="!"
                  spwd.SetAt(0, CChar("_"))
            End If
      End If
End Sub
```

To use a custom script for generating a password

1. Create your script in the category **Script Library** in the Designer.
2. Edit the password policy.
    a. Select the category **Cloud Target Systems | Basic configuration data | Password policies** in the Manager.
    b. Enter the name of the script to generate a password in **Generation script** on the **Scripts** tab.
    c. Save the changes.

Related Topics

- Script for Checking a Password on page 56

Restricted Passwords

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

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

To add a term to the restricted list

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

Testing a Password

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

To test whether a password conforms to the password policy

1. Select the category **Cloud Target Systems | Basic configuration data | Password policies** in the Manager.
2. Select the **Test** tab.
3. Select the table and object to be tested in **Base object for test**.
4. Enter a password in **Enter password to test**.

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

Testing Generating a Password

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

To generate a password that conforms to the password policy

1. Select the category **Cloud Target Systems | Basic configuration data | Password policies** in the Manager.
2. Select the **Test** tab.
3. Click **Generate**.

   This generates and displays a password.

Assigning a Password Policy

The password policy "Cloud system password policy" is predefined for cloud target systems. You can apply this password policy to cloud target system user account passwords (`CSMUser.Password`) or to a container.

If the cloud target systems' or containers' password requirements differ, it is recommended that you set up your own password policies for each cloud target system or container.

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

To reassign a password policy

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

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

Table 20: Assigning a Password Policy

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

5. Save the changes.

To change a password policy's assignment

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

Initial Password for New User Accounts

Table 21: Configuration Parameters for Formatting Initial Passwords for User Accounts

Configuration parameter	Meaning
QER\Person\UseCentralPassword	This configuration parameter specifies whether the employee's central password is used in the user accounts. The employee's central

Configuration parameter	Meaning
	password is automatically mapped to the employee's user account in all permitted target systems. This excludes privileged user accounts, which are not updated.
QER\Person\UseCentralPassword\PermanentStore	This configuration parameter controls the storage period for central passwords. If the parameter is set, the employee's central password is permanently stored. If the parameter is not set, the central password is only to publicize the target system and is subsequently deleted from the One Identity Manager database.
TargetSystem\CSM\Accounts\InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.

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

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

    If the configuration parameter "QER\Person\UseCentralPassword" is set, the employee's central password is automatically mapped to an employee's user account in each of the target systems. This excludes privileged user accounts, which are not updated.

- Use the configuration parameter "QER\Person\UseCentralPassword\PermanentStore" in the Designer to specify whether an employee's central password is permanently saved in the One Identity Manager database or only until the password has been published in the target system.

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

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

- Create user accounts manually and enter a password in their master data.
- Specify an initial password to be used when user accounts are created automatically.
  - Apply the target system specific password policies and enter an initial password in the password policies.
- Assign a randomly generated initial password to enter when you create user accounts.
  - Set the configuration parameter "TargetSystem\CSM\Accounts\InitialRandomPassword" in the Designer.
  - Apply target system specific password policies and define the character sets that the password must contain.
  - Specify which employee will receive the initial password by email.

Related Topics

- Password Policies on page 52
- Email Notifications about Login Data on page 62

Email Notifications about Login Data

Table 22: Configuration Parameters for Notifications about Login Data

Configuration parameter	Meaning
TargetSystem\CSM\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\CSM\DefaultAddress".
TargetSystem\CSM\Accounts\	This configuration parameter contains the name of the

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

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

To use email notifications about login data

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

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

To send initial login data by email

1. Set the configuration parameter "TargetSystem\CSM\Accounts\InitialRandomPassword" in the Designer.
2. Set the configuration parameter "TargetSystem\CSM\Accounts\InitialRandomPassword\SendTo" in the Designer and enter the message recipient as the value.
3. Set the configuration parameter "TargetSystem\CSM\Accounts\InitialRandomPassword\SendTo\MailTemplateAccountName" in the

Designer.

By default, the message sent uses the mail template "Employee - new account created". The message contains the name of the user account.

4. Set the confiugration parameter "TargetSystem\CSM\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword" in the Designer.

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

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

Target System Managers

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

Implementing Application Roles for Target System Managers

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

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

Table 23: Default Application Roles for Target System Managers

User	Task
Target System Managers	Target system managers must be assigned to the application role **Target systems | Cloud target systems** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare groups for adding to the IT Shop.

User	Task
	• Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects. • Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

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

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

1. Log yourself into the Manager as target system administrator (application role **Target systems | Administrator**).
2. Select the category **One Identity Manager Administration | Target systems | Cloud target systems**.
3. Select **Assign employees** in the task view.
4. Assign the employees you want and save the changes.

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

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

To define target system managers for individual cloud target systems.

1. Login to the Manager as target system manager.
2. Select the category **Cloud Target Systems | Basic configuration data | Cloud target systems**.
3. Select the target system in the result list.
4. Select **Change master data** in the task view.

5. Select the application role on the **General** tab in the **Target system manager** menu.

   - OR -

   Click next to the **Target system manager** menu to create a new application role.

   - Enter the application role name and assign the parent application role **Target systems | Cloud target systems**.
   - Click **OK** to add the new application role.

6. Save the changes.
7. Assign the application role to employees, who are authorized to edit the target system in One Identity Manager.

Related Topics

- One Identity Manager Users for Managing Cloud Target Systems on page 8
- General Master Data for a Cloud Target System on page 71
- Container Structures in a Cloud Target System on page 76

Editing a Server

In order to handle One Identity Manager specific processes in Universal Cloud Interface, the synchronization server and its server functionality must be declared. You have several options for defining a server's functionality:

- Create an entry for the Job server in the category **Base Data | Installation | Job server** in the Designer. For detailed information, see the One Identity Manager Configuration Guide.
- Select an entry for the Job server in the category **Cloud Target Systems | Basic configuration data | Server** in the Manager and edit the Job server master data.

  Use this task if the Job server has already been declared in One Identity Manager and you want to configure special functions for the Job server.

NOTE: One Identity Manager must be installed, configured and started in order for a server to execute its function in the One Identity Manager Service network. Proceed as follows in the One Identity Manager Installation Guide.

To edit a Job server and its functions

1. Select the category **Cloud Target Systems | Basic configuration data | Servers** in the Manager.
2. Select the Job server entry in the result list.
3. Select **Change master data** in the task view.
4. Edit the Job server's master data.

5. Select **Assign server functions** in the task view and specify server functionality.
6. Save the changes.

Detailed information about this topic

- Master Data for a Job Server on page 67
- Specifying Server Functions on page 69

Related Topics

- Setting Up the Synchronization Server on page 13

Master Data for a Job Server

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

Table 24: Job Server Properties

Property	Meaning
Server	Job server name.
Full server name	Full server name in accordance with DNS syntax. Example: `<Name of servers>.<Fully qualified domain name>`
Target System	Computer account target system.
Language culture	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The properties **Server is cluster** and **Server belongs to cluster** are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.

Property	Meaning
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. Only the methods "Robocopy" and "Rsync" are currently supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication then takes place between servers with a Windows operating system using "Robocopy" and between servers with the Linux operating system using "rsync". If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when One Identity Manager Service is automatically updated. If the server is handling several queues the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. Permitted values are "Win32", "Windows", "Linux" and "Unix". If the input is empty, "Win32" is assumed.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server) the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain and the service account password have to be entered for the server.
One Identity Manager	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.

Property	Meaning
Service installed	The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in program "Job Queue Info".
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently being executed.
Server Function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related Topics

- Specifying Server Functions on page 69

Specifying Server Functions

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

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled depending on the server function.

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

Table 25: Permitted Server Functions

Server Function	Remark
Update Server	This server executes automatic software updating of all other servers. The server requires a direct connection to the database server that the One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled

Server Function	Remark
	with this functionality during initial installation of the schema.
SQL processing server	This server can process SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
SMTP host	Server from which the One Identity Manager Service sends email notifications. Prerequisite for sending mails using the One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
Universal Cloud Interface connector	The server can connect to the Universal Cloud Interface Module.

Related Topics

- Master Data for a Job Server on page 67

4

Cloud Target Systems

A cloud target system corresponds to a cloud application in the Universal Cloud Interface.

NOTE: Use One Identity Manager set ups the cloud target system in the Synchronization Editor database.

To edit a cloud system's master data

1. Select the category **Cloud Target Systems | Basic configuration data | Cloud target systems**.
2. Select a target system in the result list. Select **Change master data** in the task view.
3. Edit the target system type master data.
4. Save the changes.

TIP: You can also edit cloud target system properties in the category **Cloud Target Systems | <target system>**.

Detailed information about this topic

- General Master Data for a Cloud Target System on page 71
- Specifying Categories for Inheriting Groups on page 74
- Alternative Column Names on page 74

General Master Data for a Cloud Target System

Enter the following master data for a cloud target system.

Table 26: Cloud Target System Master Data

Property	Description
Cloud target system	Name of the target system.
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	Cloud 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 cloud target system and user accounts should be created which are already managed (state "linked configured"). The account definition's default manage level is applied. User accounts are only linked to the employee (state "Linked") if no account definition is given. This is the case on initial synchronization, for example.
Target system managers	Application role in which target system managers are specified. The target system managers only modify the cloud target system objects assigned to them. Therefore, each cloud target system can have a different target system manager assigned to it. Select the One Identity Manager application role whose members are responsible for administration of this cloud target system. Use the button to add a new application role.
Synchronized by	NOTE: You can only specify the synchronization type when adding a new cloud target system. No changes can be made after saving. "One Identity Manager" is used when you create a cloud target system with the Synchronization Editor. Type of synchronization through which the data is synchronized between the target system and One Identity Manager.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td></td><td>
Table 27: Permitted Values
<table>
<tr><th>Value</th><th>Synchronization by</th><th>Provisioned by</th></tr>
<tr><td>One Identity Manager</td><td>Universal Cloud Interface connector</td><td>Universal Cloud Interface connector</td></tr>
<tr><td>No synchron-ization</td><td>none</td><td>none</td></tr>
</table>
NOTE: If you select "No synchronization" you can define custom processes to exchange data between One Identity Manager and the target system.
</td></tr>
<tr><td>Description</td><td>Spare text box for additional explanation.</td></tr>
<tr><td>Manual provisioning</td><td>Specifies whether changes to cloud objects in the One Identity Manager database are automatically provisioned in the cloud application. If this option is not set, processes for automatic provisioning of object modifications are configured.
Set this option, if object modifications are not allowed to be published automatically in the cloud application. Use the Web Portal to transfer the changes to the cloud application. For more detailed information about provisioning object modifications, see the One Identity Manager Administration Guide for Connecting to Cloud Applications.
IMPORTANT: If you set this option, ensure that data, using regular and frequent synchronization,
• between the Universal Cloud Interface Module and the cloud application
• between the Universal Cloud Interface module and Cloud Systems Management
is kept consistent!</td></tr>
<tr><td>User account deletion not permitted</td><td>Specifies whether user accounts in the cloud target system can be deleted. If this option is set, user account can only be disabled.</td></tr>
</table>

Related Topics

- Automatic Assignment of Employees to User Accounts on page 91
- Target System Managers on page 64

Specifying Categories for Inheriting Groups

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

To define a category

1. Select the category **Cloud Target Systems | Basic configuration data | Cloud target systems**.
2. Select a target system in the result list.
3. Select **Change master data** in the task view.
4. Switch to the **Mapping rule category** tab.
5. Expand the respective base node of the user account or group table.
6. Click to enable category.
7. Enter a name for the user account and group categories in the current language.
8. Save the changes.

Detailed information about this topic

- Group Inheritance Based on Categories on page 110

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

4. Open the membership tree in the table whose column name you want to change.

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

How to Edit a Synchronization Project

Synchronization projects, in which a cloud target system is already used as a base object, can also be opened using the Manager. You can, for example, check the configuration or view the synchronization log in this mode. The Synchronization Editor is not started with its full functionality. You cannot run certain functions, such as, running synchronization or simulation, starting the target system browser and others.

NOTE: The Manager is locked for editing throughout. To edit objects in the Manager, close the Synchronization Editor.

To open an existing synchronization project in the Synchronization Editor

1. Select the category **Cloud Target Systems | Basic configuration data | Cloud target systems**.
2. Select a target system in the result list. Select **Change master data** in the task view.
3. Select **Edit synchronization project...** from the task view.

Related Topics

- Customizing Synchronization Configuration on page 25

Container Structures in a Cloud Target System

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

To edit container master data

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

   - OR -

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

Enter the following master data for a container.

Table 28: Master Data for a Container

Property	Description
Name	Container name.
Distinguished name	Container's distinguished name.
Parent container	Parent container for mapping a hierarchical container structure.
Cloud target system	The container's cloud target system.
Description	Spare text box for additional explanation.
Account manager	Manager responsible for the container. ***To specify an account manager***

Property	Description
	1. Click → next to the text box. 2. Under **Table**, select the table which maps the account manager. 3. Select the manager under **Account manager**. 4. Click **OK**.
Target system managers	Application role in which target system managers are specified for the container. Target system managers only edit container objects that are assigned to them. Each container can have a different target system manager assigned to it. Select the One Identity Manager application role whose members are responsible for administration of this container. Use the button to add a new application role.

Related Topics

- Target System Managers on page 64

6

Cloud User Accounts

You manage cloud application user accounts with One Identity Manager. User accounts obtain the permissions required to access cloud resources through membership in groups and permissions controls.

Detailed information about this topic

Linking User Accounts to Employees

The central component of the One Identity Manager is to map employees and their master data with permissions through which they have control over different target systems. For this purpose, information about user accounts and permissions can be read from the target system into the One Identity Manager database and linked to employees. This gives an overview of the permissions for each employees in all of the connected target systems. One Identity Manager provides the possibility to manage user accounts and their permissions. You can provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

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

- Employees and user accounts can be entered manually and assigned to each other.
- Employees can automatically obtain their account definitions using user account resources. If an employee does not have a user account in a target system, a new user account is created. This is done by assigning account definitions to an employee using the integrated inheritance mechanism followed by process handling.

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

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

- An existing employee is automatically assigned when a user account is added or a new employee is created if necessary. In this case, employee master data is created on the basis of the existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. This method, however, is not the One Identity Manager default method. Define criteria for finding employees for automatic employee assignment.

Related Topics

- Entering Master Data for User Accounts on page 82
- Setting Up Account Definitions on page 34
- Automatic Assignment of Employees to User Accounts on page 91

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

Supported User Account Types

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

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

- Identity (column `IdentityType`)

  The identity describes the type of user account.

Table 29: Identities of User Accounts

Identity	Description	Value of the column "IdentityType"
Primary identity	Employee's default user account.	Primary
Organizational identity	Secondary user account used for various roles within the organization, f. ex. In sub-agreements with other functional areas.	Organizational

Identity	Description	Value of the column "IdentityType"
Personalized admin identity	User account with administration rights used by one person.	Admin
Sponsored identity	User account used for example for training purposes.	Sponsored
Shared identity	User account with administration rights used by several people.	Shared
Service identity	Service account.	Service

- Privileged user account (column `IsPrivilegedAccount`)

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

Default User Accounts

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

To create default user accounts through account definitions

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

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

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

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

4. Enter the effective IT operating data for the target system. Select the concrete target system under **Effects on**.

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

5. Assign the account definition to employees.

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

Administrative User Accounts

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

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

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

Privileged User Accounts

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

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

To create privileged users through account definitions

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

   An account definition specifies which rules are used to generate the IT operating data for example, whether the container for a user account is made up of the employee's

department, cost center, location or business role and which default values will be used if no IT operating data can be found through the employee's primary roles.

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

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

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

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

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

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

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

Entering Master Data for User Accounts

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

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

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

To edit master data for a user account

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

   - OR-

   Click in the result list toolbar.

3. Edit the user account's resource data.
4. Save the changes.

To manually assign or create a user account for an employee

1. Select the **Employees | Employees**.
2. Select the employee in the result list and run **Assign cloud user accounts** from the task view.
3. Assign a user account.
4. Save the changes.

Detailed information about this topic

- Additional Master Data for a User Account on page 83
- User Account Login Data on page 86
- Identification Tasks on page 87
- Contact Data on page 88
- User Defined Master Data on page 88

Related Topics

- Deleting User Accounts on page 97

Additional Master Data for a User Account

Table 30: Configuration Parameters for Setting up User Accounts

Configuration parameter	Active Meaning
QER\CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is set, a value for the risk index can be entered and calculated.

Enter the following data on the **General** tab:

Table 31: 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

Property	Description
	account manually, you can select an employee in the menu. If you use automatic employee assignment, an associated employee is created and entered into the user account when the user account is saved.
Target System	The user account's cloud target system.
Account definition	Account definition through which the user account was created. Use the account definition to automatically fill user account master data and to specify a manage level for the user account. The One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account. NOTE: The account definition cannot be changed once the user account has been saved.
Manage level	User account's manage level. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
Form of address	Employee's form of address.
First name	The user's first name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Last name	The user's last name. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Full name	Full name of the user account.
Initials	The user's initials. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Job description	The user's job description. If you have assigned an account definition, the input field is automatically filled out with respect to the manage level.
Nickname	Additional information about the user account.
Surname prefix	A prefix to the user's surname, for example "von" or "de".
Display name	User account display name.
Alias	Alias for further identification of the user account.
Name	User account identifier.
Container	Container in which to create the user account. If you have assigned an

Property	Description
	account definition, the container is determined from the company IT data for the assigned employee depending on the manage level of the user account.
First primary group	User account's primary group.
Second primary group	Additional primary group for the user account. If there group with different groups types in the target system, you can assign another primary group here.
Email address	User account's email address.
Email encoding	Type of email encoding.
Account expiry date	The date from which the user account can no longer be used to log in. If you specify a leaving date for an employee it is used as account expiry date if the appropriate manage level is set. Any existing account expiry date is overwritten in this case. NOTE: If the employee's leaving date is deleted at a later point in time, the user account expiry date remains intact!
Resource type	Type of the resource, for example, `user`.
Risk index (calculated)	Maximum risk index values for all assigned groups. This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.
Category	Categories for the inheritance of groups by the user account. Select one or more categories from the menu. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories.
Description	Spare text box for additional explanation.
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.
Identity	User account's identity type

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td></td><td>Table 32: Permitted values for the identity.
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>Primary identity</td><td>Employee's default user account.</td></tr>
<tr><td>Organizational identity</td><td>Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas.</td></tr>
<tr><td>Personalized admin identity</td><td>User account with administrative permissions, used by one employee.</td></tr>
<tr><td>Sponsored identity</td><td>User account that is used for training purposes, for example.</td></tr>
<tr><td>Shared identity</td><td>User account with administrative permissions, used by several employees.</td></tr>
<tr><td>Service identity</td><td>Service account.</td></tr>
</table></td></tr>
<tr><td>Privileged user account</td><td>Specifies whether this is a privileged user account.</td></tr>
<tr><td>Groups can be inherited</td><td>Specifies whether the user account groups can inherit through the employee. If this option is set, the user account inherits groups through hierarchical roles or IT Shop requests.
If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups.
If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.</td></tr>
<tr><td>User account is disabled</td><td>Specifies that the user account is locked. If a user account is not required for a period of time, you can temporarily disable the user account by using the option <User account is deactivated>.</td></tr>
</table>

Related Topics

- Locking and Unlocking User Accounts on page 96

User Account Login Data

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.

Enter the following master data on the **Login** tab.

Table 33: User Account Login Data

Property	Description
Password/Password confirmation	Password for the user account. Depending on the configuration parameter "Person\UseCentralPassword" the employee's central password can be mapped to the user account's password. If you use an initial password for the user accounts, it is automatically entered when a user account is created.
Password last changed	Date on which the password was last changed.
Last login	Date and time of the last login to the cloud application.

Related Topics

- Password Policies on page 52

Identification Tasks

You can find an employee's address information used by this user account, on the **Identification** tab.

Table 34: Identification Data for a User Account

Property	Description
Street	Street or road.
Mailbox	Mailbox.
Town	City.
Zip code	Zip code.
State	State.
Country	Country.
Address	Formatted postal address.
Language culture	Language and code identifier.
Time zones	Timezone identifier.
Room	Room.
Department	Employee's department

Property	Description
Area	Area the accounts belongs to.
Organization	Organization the accounts belongs to.
Employee number	Number for identifying the employee, in addition to their ID.
Employment	Type of job.
Account manager	Manager responsible for the user account. ***To specify an account manager*** 1. Click → next to the text box. 2. Under **Table**, select the table which maps the account manager. 3. Select the manager under **Account manager**. 4. Click **OK**.

Contact Data

You can find the information about the employee's contactability used by this user account, on the **Contact** tab.

Table 35: Contact Data for a User Account

Property	Description
Phone	Landline telephone number.
Mobile phone	Mobile telephone number.
Website	The user's website.

User Defined Master Data

You can find customized data for a user account on the **Custom** tab.

Table 36: Customized Master Data for a User Account

Property	Description
Spare fields no. 01-spare field no. 05	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Property	Description
Spare date no. 01 - spare date no. 03	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.
Spare text no. 01 - spare text no. 05	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.
Spare option no. 01 - spare option no. 05	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Additional Tasks for Managing User Accounts

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

Overview of User Accounts

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

To obtain an overview of a user account

1. Select the category **Cloud Target Systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Select **User account overview** in the task view.

Assigning Groups directly to User Accounts

Cloud groups can be assigned directly or indirectly to a user account. Indirect assignment is carried out by allocating the employee and groups in hierarchical roles, like departments, cost centers, locations or business roles. If the employee has a cloud user account, cloud groups in the hierarchical roles are inherited by this user account.

To assign groups directly to user accounts

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

   The view- OR -

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

NOTE: The user account's primary group is already assigned and labeled as "Not yet applied". Edit the user account's master data to change its primary group.

Related Topics

- Assigning Groups to User Accounts on page 102

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 **Cloud 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.

Assigning Extended Properties

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

To specify extended properties for a user account

1. Select the category **Cloud Target Systems | <target system> | User accounts**.
2. Select the user account in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   - OR -

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

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

Automatic Assignment of Employees to User Accounts

Table 37: Configuration Parameters for Synchronizing a Cloud Application

Configuration parameter	Meaning
TargetSystem\CSM\PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem\CSM\PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.
TargetSystem\CSM\PersonAutoFullSync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\CSM\PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names given in a pipe (|) delimited list that is handled as a regular search pattern.

When you add a user account, an existing employee can be assigned automatically or added if necessary. In the process, the employee master data is created based for existing

user master data. This mechanism can follow on after a new user account has been created manually or through synchronization. Define criteria for finding employees to apply to automatic employee assignment. If a user account is linked to an employee through the current mode, the user account is given, through an internal process, the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

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

Run the following tasks to assign employees automatically.

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

  Example:

  `ADMINISTRATOR`
- Assign an account definition to the cloud target system. Ensure the manage level to be used is entered as default automation level.
- Define the search criteria for employees assigned to the cloud target system.

NOTE:

The following applies for synchronization:

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

The following applies outside synchronization:

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

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

To select user accounts through account definitions

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

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

Related Topics

- Creating an Account Definition on page 35
- Assigning Account Definitions to a Cloud Target System on page 49
- Editing Search Criteria for Automatic Employee Assignment on page 93

Editing Search Criteria for Automatic Employee Assignment

Criteria for employee assignment are defined in the target systems. In this case, you specify which user account properties must match the employee's properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criteria are written in XML notation in the column "Search criteria for automatic employee assignment" (`AccountToPersonMatchingRule`) of the `CSMRoot` table.

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

NOTE: When the employees are assigned to user accounts on the basis of search criteria, user accounts are given the default manage level of the account definition entered in the user account's target system. You can customize user account properties depending on how the behavior of the manage level is defined.

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

To define employee assignment criteria for a cloud target system

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

   Table 38: Example of Search Criteria for User Accounts

Employee column	User account column	
Cloud user account	First name (FirstName) AND last name (LastName)	First name (FirstName) AND last name (LastName)

5. Save the changes.

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

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

Table 39: Manual Assignment View

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

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

To apply search criteria to user accounts

- Click **Reload**.

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

To assign employees directly over a suggestion list

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

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

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

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

To remove assignments

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

      The assigned employees are deleted from the selected user accounts.

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

Related Topics

- Automatic Assignment of Employees to User Accounts on page 91

Locking and Unlocking User Accounts

Table 40: Configuration Parameter for Disabling User Accounts

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

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

Scenario:

- The user account is linked to employees and is managed through account definitions.

User accounts managed through account definitions are disabled when the employee is temporarily or permanently disabled. The behavior depends on the user account manage level. User accounts with the manage level "Full managed" are disabled depending on the account definition settings. For user accounts with another manage level, modify the column template `CSMUser.AccountDisabled` accordingly.

Scenario:

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

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

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

To lock a user account when the configuration parameter is disabled

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

Scenario:

- User accounts not linked to employees.

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

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

Related Topics

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

- Setting Up Account Definitions on page 34
- Setting Up Manage Levels on page 37

Deleting User Accounts

You can delete a user account from the result list or the menu base. After the deletion has been confirmed, the user account is deleted from the One Identity Manager database.

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 deletion delay on the table `CSMUser` in the Designer.

To delete a user account

1. Select the category **Cloud 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**.

Once you have deleted a user account, it is also deleted in the Universal Cloud Interface Module through the provisioning process and then in the cloud application. The deletion is logged as a pending change. You can see whether the user account has been deleted in the cloud application from the process status for the pending change. The same applies if memberships of user accounts in groups are deleted.

User accounts are not allowed to be deleted in certain cloud applications. These user accounts cannot be deleted in the Manager, only disabled. You can configure the appropriate behavior in the cloud target system.

To prevent user accounts from being deleted

1. Select the category **Cloud Target Systems | Basic configuration data | Cloud target systems**.
2. Select a target system in the result list. Select **Change master data** in the task view.
3. Set the option **User account deletion not permitted**.
4. Save the changes.

Detailed information about this topic

- Provisioning Object Changes on page 118
- General Master Data for a Cloud Target System on page 71
- Locking and Unlocking User Accounts on page 96

7

Cloud Groups

Groups map the objects that control access to cloud resources though the cloud application. A user account obtains access permissions to cloud resources through its group memberships.

To edit group master data

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

   - OR -

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

Detailed information about this topic

- Entering Master Data for a Group on page 99
- User Defined Master Data for an Group on page 101

Entering Master Data for a Group

Table 41: Configuration Parameters for Setting up User Accounts

Configuration parameter	Active Meaning
QER\CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is set, a value for the risk index can be entered and calculated.

Enter the following master data for a group.

Table 42: Entering Master Data for a Group

Property	Description
Name	Group identifier
Container	Container in which to create the group.
Target System	The group's cloud target system
Distinguished name	Distinguished name of the group.
Display name	The display name is used to display the group in the One Identity Manager tools user interface.
Group name	Additional name for the group.
Email address	Group's email address
Account manager	Manager responsible for the group. ***To specify an account manager*** 1. Click → next to the text box. 2. Under **Table**, select the table which maps the account manager. 3. Select the manager under **Account manager**. 4. Click **OK**.
IT Shop	Specifies whether the group can be requested through the IT Shop. This group can be requested by staff through the Web Portal and granted through a defined approval process. The group can still be assigned directly to hierarchical roles. For more detailed information, see the One Identity Manager IT Shop Administration Guide.
Only for use in IT Shop	Specifies whether the group can only be requested through the IT Shop. This group can be requested by staff through the Web Portal and granted through a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is no permitted.
Service item	Service item data for requesting the group through the IT Shop.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.
Notes	Categories for group inheritance. Groups can be selectively inherited by

Property	Description
category	user accounts. To do this, groups and user accounts are divided into categories. Use this menu to allocate one or more categories to the group. For more detailed information, see the One Identity Manager Target System Base Module Administration Guide.
Description	Spare text box for additional explanation.
Group type	Name of the group type. This is only required if different group types are recognized in the cloud application.
Resource type	Type of resource, for example, `Group`.

Detailed information about this topic

- Specifying Categories for Inheriting Groups on page 74

User Defined Master Data for an Group

You can find customized data for a group on the **Custom** tab.

Table 43: User Defined Master Data for an Group

Property	Description
Spare fields no. 01- spare field no. 05	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.
Spare date no. 01 - spare date no. 03	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.
Spare text no. 01 - spare text no. 05	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.
Spare option no. 01 - spare option no. 05	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Assigning Groups to User Accounts

cloud groups can be assigned directly or indirectly to employees. In the case of indirect assignment, employees and groups are arranged in hierarchical roles. The number of groups assigned to an employee is calculated from the position in the hierarchy and the direction of inheritance. If you add an employee to hierarchical roles and that employee owns a cloud user account, this user account is added to the cloud group. Prerequisites for indirect assignment of employees to user accounts:

- Assignment of employees and cloud groups is permitted for role classes (department, cost center, location or business role).
- Cloud user accounts are marked with the option **Groups can be inherited**.
- Cloud user accounts and cloud groups belong to the same target system.

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

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

Detailed information about this topic

- Assigning Groups to Departments, Cost Centers and Locations on page 102
- Assigning Groups to Business Roles on page 103
- Assigning User Accounts to a Group on page 104
- Adding Groups to System Roles on page 105
- Adding Groups to the IT Shop on page 106

Assigning Groups to Departments, Cost Centers and Locations

Assign groups to departments, cost centers and locations in order to assign user accounts to them through these organizations.

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

1. Select the category **Cloud Target Systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign organizations**.
4. Assign organizations in **Add assignments**.

- Assign departments on the **Departments** tab.
- Assign locations on the **Locations** tab.
- Assign cost centers on the **Cost center** tab.

- OR -

Remove the organizations from **Remove assignments**.

5. Save the changes.

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

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

   - OR -

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

   - OR -

   Select the category **Organizations | Locations**.
2. Select the department, cost center or location in the result list.
3. Select **Assign Cloud groups.**
4. Assign groups in **Add assignments**.

   - OR -

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

Related Topics

- Assigning Groups to Business Roles on page 103
- Assigning User Accounts to a Group on page 104
- Adding Groups to System Roles on page 105
- Adding Groups to the IT Shop on page 106
- One Identity Manager Users for Managing Cloud Target Systems on page 8

Assigning Groups to Business Roles

Installed Modules: Business Roles Module

You assign groups to business roles in order to assign them to user accounts over business roles.

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

1. Select the category **Cloud Target Systems | <target system> | Groups**.
2. Select the group in the result list.

3. Select **Assign business roles** in the task view.
4. Assign business roles in **Add assignments**.

   - OR -

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

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

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

   - OR -

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

Related Topics

- Assigning Groups to Departments, Cost Centers and Locations on page 102
- Assigning User Accounts to a Group on page 104
- Adding Groups to System Roles on page 105
- Adding Groups to the IT Shop on page 106
- One Identity Manager Users for Managing Cloud Target Systems on page 8

Assigning User Accounts to a Group

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

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

To assign a group directly to user accounts

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

   The view- OR -

Remove user accounts from **Remove assignments**.

5. Save the changes.

Related Topics

- Assigning Groups directly to User Accounts on page 89
- Assigning Groups to Departments, Cost Centers and Locations on page 102
- Assigning Groups to Business Roles on page 103
- Adding Groups to System Roles on page 105
- Adding Groups to the IT Shop on page 106

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 employees' user accounts inherit the group.

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

To assign a group to system roles

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

   - OR -

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

Related Topics

- Assigning Groups to Departments, Cost Centers and Locations on page 102
- Assigning Groups to Business Roles on page 103
- Assigning User Accounts to a Group on page 104
- Adding Groups to the IT Shop on page 106

Adding Groups to the IT Shop

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

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

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

To add a group to the IT Shop

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

   - OR -

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

To remove a group from individual IT Shop shelves.

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

   - OR -

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

To remove a group from all IT Shop shelves.

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

   - OR -

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

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

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

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

Related Topics

- Entering Master Data for a Group on page 99
- Assigning Groups to Departments, Cost Centers and Locations on page 102
- Assigning Groups to Business Roles on page 103
- Assigning User Accounts to a Group on page 104
- Adding Groups to System Roles on page 105

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 **Cloud 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.

To assign groups directly to a group

1. Select the category **Cloud Target Systems | <target system> | Groups**.
2. Select the group in the result list.
3. Select **Assign groups** in the task view.
4. Assign child groups of the selected group in **Add assignments**.

   - OR -

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

Effectiveness of Group Memberships

Table 44: Configuration Parameter for Conditional Inheritance

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

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

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

NOTE:

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

The effect of the assignments is mapped in the tables `CSMUserInGroup` and `CSMBaseTreeHasGroup` through the column `XIsInEffect`.

Example of the effect of group memberships

- 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 45: Specifying excluded groups (table `CSMGroupExclusion`)

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

Table 46: 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 47: Excluded groups and effective assignments

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

Prerequisites

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

To exclude a group

1. Select the category **Cloud Target Systems | <target system> | Groups**.
2. Select a group in the result list.
3. Select **Exclude groups** in the task view.
4. Assign the groups that are mutually exclusive to the selected group in **Add assignments**.

   - OR -

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

Group Inheritance Based on Categories

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

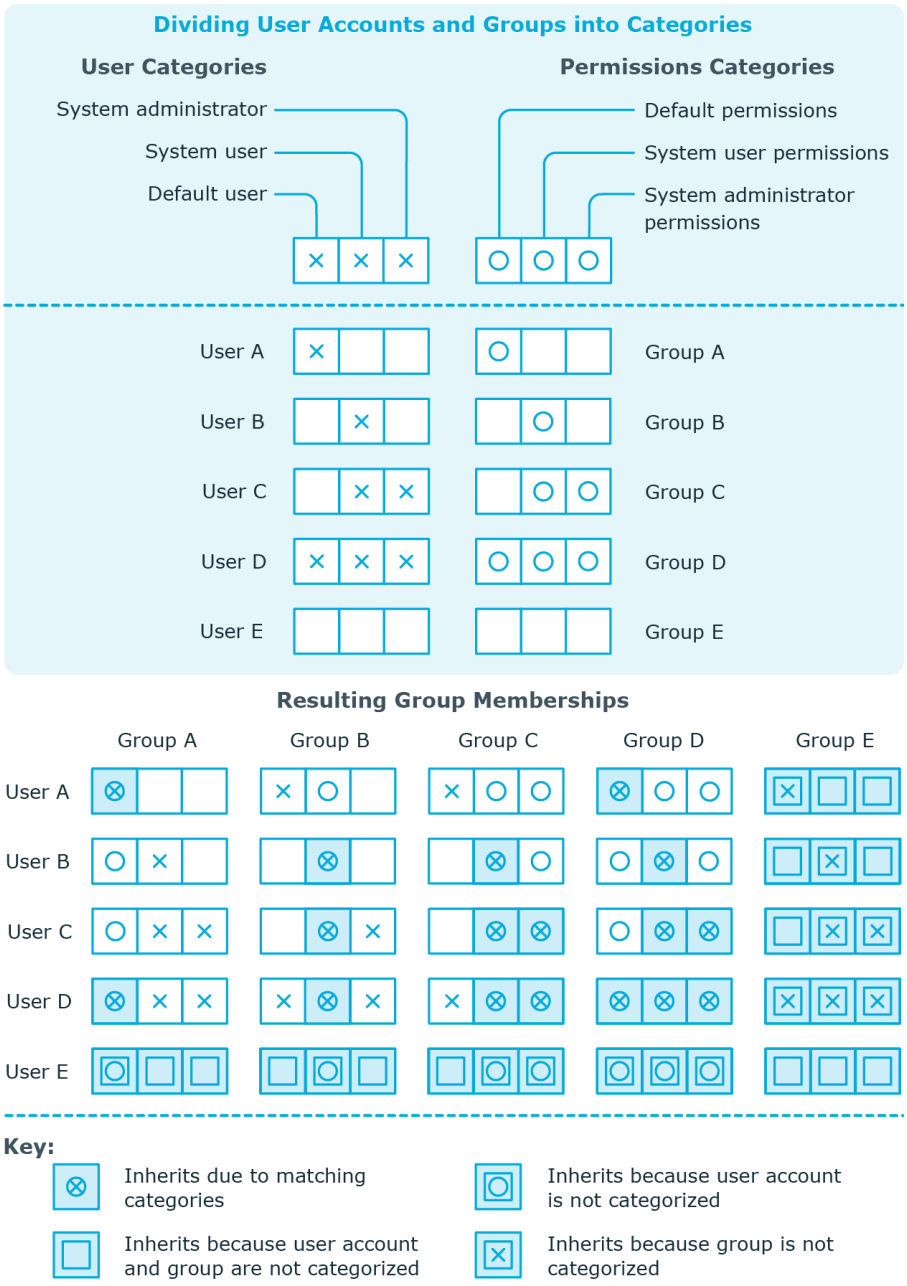
Every user account can be assigned to one or more categories. Each group can also be assigned to one or more categories. The group is inherited by the user account when at least one user account category item matches an assigned group. The group is also inherited by the user account if the group or the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

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

Table 48: 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 2: Example of inheriting through categories.



To use inheritance through categories

- Define categories in the cloud 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 74
- Additional Master Data for a User Account on page 83
- Entering Master Data for a Group on page 99

Assigning Permissions Controls

Use this task to assign permissions controls to groups.

To assign permissions controls to a group

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

   - OR -

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

Related Topics

- Cloud Permissions Controls on page 114

Assigning Extended Properties

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

To specify extended properties for a group

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

   - OR -

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

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

Deleting Groups

To delete a group

1. Select the category **Cloud Target Systems | <target system> | Groups**.
2. Select the group in the result list.
3. Click to delete the group.
4. Confirm the security prompt with **Yes**.

This deletes the group completely from the One Identity Manager database. Once you have deleted a group, it is also deleted in the Universal Cloud Interface Module through the provisioning process and then in the cloud application. The deletion is logged as a pending change. You can see whether the group has been deleted in the cloud application from the process status for the pending change. The same applies if memberships of user accounts in groups are deleted.

Related Topics

- Provisioning Object Changes on page 118

8

Cloud Permissions Controls

Use permissions controls to map more of the cloud application's properties.

To edit permissions controls

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

   - OR -

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

Detailed information about this topic

- General Master Data for Permissions Controls on page 114
- Custom Master Data for Permissions Controls on page 115

General Master Data for Permissions Controls

Enter the following master data for a permissions control.

Table 49: Permissions Control Master Data

Property	Description
Target System	Cloud target system in which the permissions control applies.
Permissions control	Name of the permissions control.

Property	Description
Access type	Additional permissions control properties.
Description	Spare text box for additional explanation.

Custom Master Data for Permissions Controls

You can find customized data for a permissions control on the **Custom** tab.

Table 50: Custom Master Data for Permissions Controls

Property	Description
Spare fields no. 01- spare field no. 05	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.
Spare date no. 01 - spare date no. 03	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.
Spare text no. 01 - spare text no. 05	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.
Spare option no. 01 - spare option no. 05	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Additional Tasks for Permissions Controls

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

Permissions Control Overview

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

To obtain an overview of a permissions control

1. Select the category **Cloud Target Systems | <target system> | Permissions controls**.
2. Select the permissions control in the result list.
3. Select **Permissions control overview** in the task view.

Assigning Permissions Controls to User Accounts

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

To assign permissions controls to user accounts

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

   The view- OR -

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

Assigning Permissions Controls to Groups

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

To assign permissions controls to groups

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

   The view- OR -

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

Deleting Permissions Controls

To delete a permissions control

1. Select the category **Cloud Target Systems | <target system> | Permissions controls**.
2. Select the permissions control in the result list.
3. Click to delete the permissions control.
4. Confirm the security prompt with **Yes**.

This deletes the permissions control completely from the One Identity Manager database. Once you have deleted a permissions control, it is also deleted in the Universal Cloud Interface Module through the provisioning process and then in the cloud application. The deletion is logged as a pending change. You can see whether the permissions control has been deleted in the cloud application from the process status for the pending change. The same applies if permissions control assignments to user accounts or groups are deleted.

Related Topics

- Provisioning Object Changes on page 118

Provisioning Object Changes

Changes to cloud objects can only be made in the Cloud Systems Management Module. Provisioning processes ensure that object changes are transferred from the Cloud Systems Management Module into the Universal Cloud Interface Module. By default, these object changes are then published in the cloud application by automatic provisioning processes.

The One Identity Manager logs the object changes as pending changes in separate tables. The table `QBMPendingChange` contains the modified objects and their processing status. The details of the changes, operations to execute, time stamp and processing status are saved in the `QBMPendingChangeDetail`.

The processing status of an object is not set to successful until all associated changes for this object have been successfully provisioned. An object's processing status is set as failed if all associated changes have been processed and at least one them has failed.

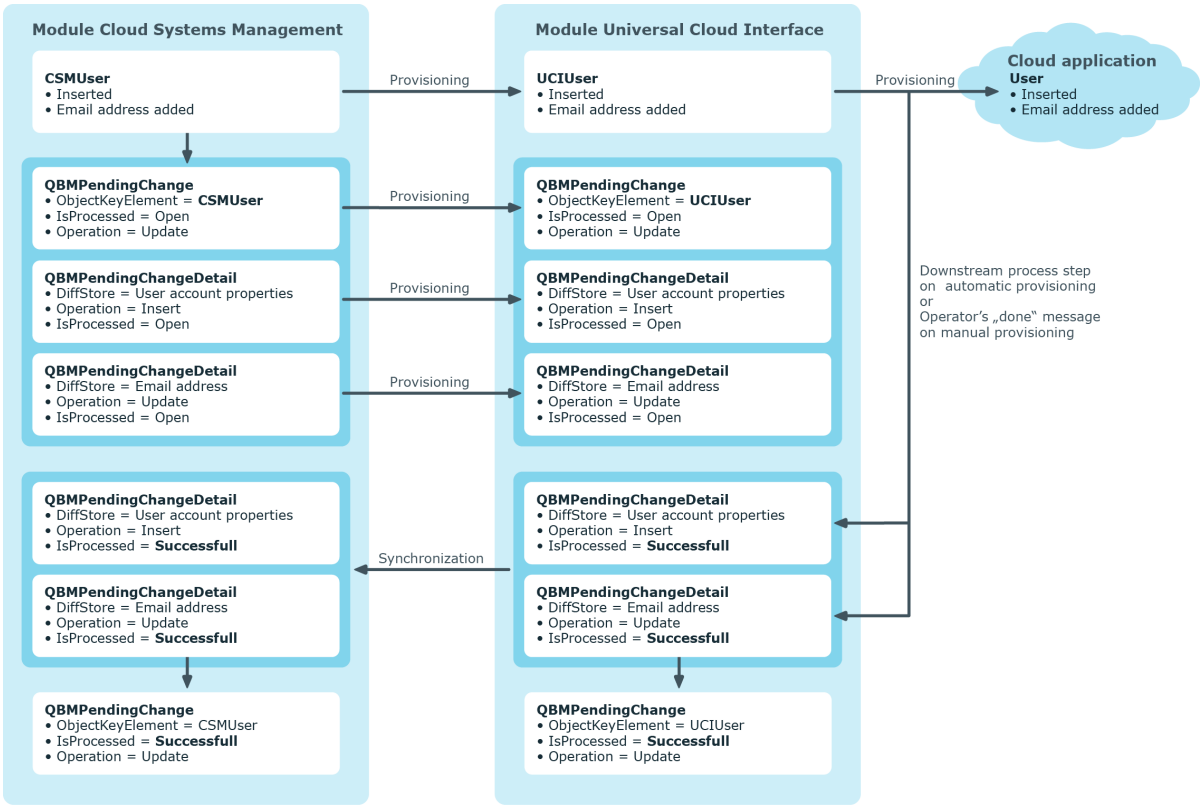
Detailed information about this topic

- The Provisioning Sequence on page 118
- Retention Time for Pending Changes on page 120

The Provisioning Sequence

The following image show how object changes are provisioned and how the pending changes associated with it are processed. The sequence does no depend on whether the module Cloud System Management and the Universal Cloud Interface are installed in the same or in separate databases.

Figure 3: Provisioning Sequence for Pending Changes



By default, the Cloud Systems Management module is synchronized hourly with the Universal Cloud Interface. This ensures that the processing state for pending changes is declared promptly in the Cloud Systems Management Module.

Displaying Pending Changes

You can view pending changes in the Manager. Here, manual and automatic provisioning processes are shown.

To display pending changes

- Select the menu item **Database | Pending changes**.

Table 51: Meaning of the Icons in the Toolbar

Icon	Meaning
	Show selected object.
	Reload the data.

Retention Time for Pending Changes

Table 52: Configuration Parameters

Configuration parameter	Effect when Set
QBM\PendingChange\LifeTimeError	This configuration parameter specifies the maximum retention period (in days) for failed provisioning processes. Default is 30 days.
QBM\PendingChange\LifeTimeRunning	This configuration parameter specifies the maximum retention period (in days) for open provisioning processes. Default is 30 days.
QBM\PendingChange\LifeTimeSuccess	This configuration parameter specifies the maximum retention period (in days) for successful provisioning processes. Default is 2 days.

Pending changes are saved for a fixed period. After expiring, the entries in `QBMPendingChange` and `QBMPendingChangeDetail` are deleted by the DBQueue Processor. The retention period depends on the status of provisioning processes and can be configured in the configuration parameter.

To configure the retention period for pending changes

1. To change the retention period for successful provisioning processes, edit the value of the configuration parameter "QBM\PendingChange\LifeTimeSuccess" in the Designer.
2. To change the retention period for failed provisioning processes, edit the value of the configuration parameter "QBM\PendingChange\LifeTimeError" in the Designer.
3. To change the retention period for open provisioning processes, edit the value of the configuration parameter "QBM\PendingChange\LifeTimeRunning" in the Designer.
4. Enter a retention period in days.

10

Reports about Objects in Cloud 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 cloud systems.

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

Table 53: Reports for the Target System

Report	Description
Overview of all Assignments (Cloud target system)	This report finds all roles containing employees with at least one user account in the selected target system.
Overview of all assignments (Cloud container)	This report finds all roles containing employees with at least one user account in the selected container.
Overview of all assignments (Cloud 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. The report contains group memberships and risk assessment.
Show employees with multiple user accounts	This report shows all employees with more than one user account in the target system. The report is a risk assessment.
Show unused user accounts	This report shows all user accounts in the target system that have not been used in the last few months. The report contains group memberships and risk assessment.
Show entitlement drifts	This report shows all target system groups, which are the result of manual operations in the target system rather than

Report	Description
	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.
Cloud target systems user account and group administration	This report contains a summary of user account and group distribution in all cloud target systems. You can find this report in the category **My One Identity Manager**.
Cloud Target Systems Data Quality Summary	This report contains different evaluations of user account data quality in all cloud target systems. You can find this report in the category **My One Identity Manager**.

Related Topics

- Overview of all Assignments on page 122

Overview of all Assignments

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

Example

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

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the report **Overview of all assignments**.

- Use the **Used by button** in the report's toolbar to select the role class (department, location, business role or IT Shop structure) for which you determine if roles exist in which there are employees with the selected base object.

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

Figure 4: Toolbar for Report "Overview of all assignments"

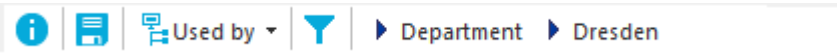


Table 54: Meaning of Icons in the Report Toolbar

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 Cloud Target Systems

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

Table 55: Configuration Parameters for Managing Cloud Target Systems

Configuration Parameter	Meaning
TargetSystem\CSM	Preprocessor relevant configuration parameter for controlling the database model components for the administration of the cloud target systems. If the parameter is set, the target system components are available. Changes to the parameter require recompiling the database.
TargetSystem\CSM\Accounts	This configuration parameter permits configuration of user account data.
TargetSystem\CSM\Accounts\InitialRandomPassword	This configuration parameter specifies whether a random generated password is issued when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem\CSM\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/busin

Configuration Parameter	Meaning
	ess 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\CSM\DefaultAddress".
TargetSystem\CSM\Accounts\ InitialRandomPassword\SendTo\ MailTemplateAccountName	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (name of the user account). Use the mail template "Employee - new account created".
TargetSystem\CSM\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	This configuration parameter contains the name of the mail template sent to inform users about their initial login data (initial password). Use the mail template "Employee - initial password for new user account".
TargetSystem\CSM\Accounts\MailTemplateDefaultValues	This configuration parameter contains the mail template used to send notifications if default IT operating data mapping values are used for automatically creating a user account. Use the mail template "Employee - new user account with default properties created".
TargetSystem\CSM\Accounts\ PrivilegedAccount	This configuration parameter allows configuration of settings for privileged user accounts.
TargetSystem\CSM\Accounts\ PrivilegedAccount\ SAMAccountName_Postfix	This configuration parameter contains the postfix for formatting login names for privileged user accounts.
TargetSystem\CSM\Accounts\ PrivilegedAccount\ SAMAccountName_Prefix	This configuration parameter contains the prefix for formatting login names for privileged user accounts.

Configuration Parameter	Meaning
TargetSystem\CSM\DefaultAddress	The configuration parameter contains the recipient's default email address for sending notifications about actions in the target system.
TargetSystem\CSM\ MaxFullsyncDuration	This configuration parameter contains the maximum runtime for synchronization. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem\CSM\PersonAutoDefault	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem\CSM\PersonAutoDisabledAccounts	This configuration parameters specifies whether employees are automatically assigned to disable user accounts. User accounts do not obtain an account definition.
TargetSystem\CSM\PersonAutoFullSync	This configuration parameter specifies the mode for automatic employee assignment for user accounts added to or updated in the database through synchronization.
TargetSystem\CSM\PersonExcludeList	List of all user accounts for which automatic employee assignment should not take place. Names given in a pipe (|) delimited list that is handled as a regular search pattern.

Appendix: Default Project Template for Cloud Application in the Universal Cloud Interface

A default project template ensures that all required information is added in the One Identity Manager. This includes mappings, workflows and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the .Synchronization Editor

The template uses mappings for the following schema types.

Table 56: Mapping Universal Cloud Interface schema types to tables in the One Identity Manager schema.

Schema type in Universal Cloud Interface	Table in the One Identity Manager schema
UCIRoot	CSMRoot
UCIContainer	CSMContainer
UCIGroup	CSMGroup
UCIGroupInGroup	CSMGroupInGroup
UCIGroupHasItem	CSMGroupHasItem
UCIItem	CSMItem
UCIUser	CSMUser
UCIUserInGroup	CSMUserInGroup
UCIUserHasItem	CSMUserHasItem
QBMPendingChange	QBMPendingChange
QBMPendingChangeDetail	QBMPendingChangeDetail

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

I

J

L

N

O

P

R

S

T

U