ONE IDENTITY™

One Identity Manager 8.1.2

Administration Guide for Connecting to a Universal Cloud Interface

Contents

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 One Identity Starling Connect cloud solution 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 exist 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 provided on an external database server.

Figure 1: Architecture for synchronization
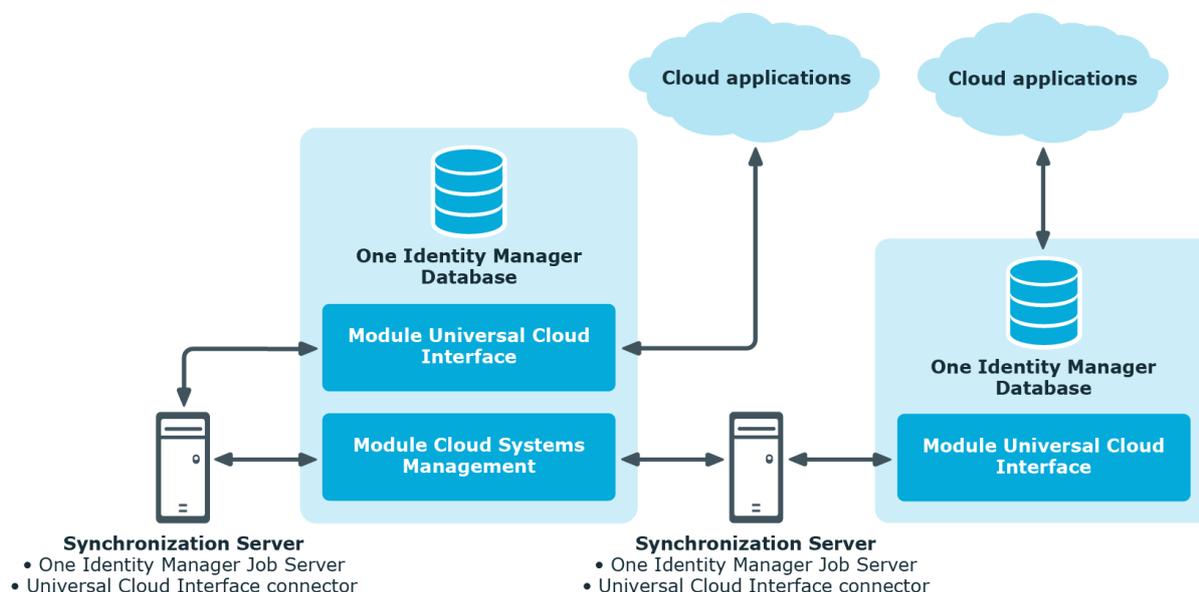
For more detailed information about communicating between the Universal Cloud Interface and cloud application, see the One Identity Manager Administration Guide for Connecting to Cloud Applications.

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	Tasks
Target system administrators	Target system administrators must be assigned to the **Target systems	Administrators** application role.
	Users with this application role:
	- Administrate application roles for individual target systems types. - Specify the target system manager. - Set up other application roles for target system managers if required. - Specify which application roles for target system managers are mutually exclusive. - 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 **Target systems	Cloud target systems** application role or a child application role.
	Users with this application role:
	- Assume administrative tasks for the target system. - Create, change, or delete target system objects, like user accounts or groups. - Edit password policies for the target system. - Prepare groups for adding to the IT Shop. - Can add employees, who have an other identity than the **Primary identity**. - Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. - Edit the synchronization's target system types and outstanding objects. - Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
One Identity Manager administrators	Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required.

ⓘNE IDENTITY™

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

Setting up synchronization with a cloud application in 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 Default project template for cloud applications in the Universal Cloud Interface on page 131.

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 "TargetSystem | CSM" configuration parameter is set.

   - In the Designer, check if the configuration parameter is set. 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

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 One Identity Manager Service requires permissions to carry out operations at file level, for example, assigning permissions and creating and editing directories and files.

User	Permissions
	The user account must belong to the **Domain users** group.
	The user account must have the **Login as a service** extended user permissions.
	The user account requires access rights to the internal web service.
	NOTE: If One Identity Manager Service runs under the network service (**NT Authority\NetworkService**), you can issue access permissions 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 One Identity Manager.
	In the default installation, 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 **Synchronization** default system user is provided for executing synchronization with 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 **Select installation modules with existing database**.
        2. Select the **Server | Job server** machine role.

    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 One Identity Manager Service to install the Server Installer. The program executes the following steps:

- Sets up a Job server.
- Specifies machine roles and server function for the Job server.
- Remotely installs One Identity Manager Service components corresponding to the machine roles.
- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. In the default case, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For detailed information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

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 remotely install the One Identity Manager Service, you must have an administrative workstation on which the One Identity Manager components are installed. For detailed information about installing a workstation, see the *One Identity Manager Installation Guide*.

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

1. Start the program Server Installer on your administrative workstation.
2. Enter the valid connection credentials for the One Identity Manager database on the **Database connection** page.
3. Specify the server on which you want to install One Identity Manager Service on the **Server properties** page.

   a. Select a Job server from the **Server** menu.

      - OR -

      To create a new Job server, click **Add**.

   b. Enter the following data for the Job server.

      - **Server**: Name of the Job server.
      - **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.
      - **Full server name**: Full server name in accordance with DNS syntax.

        Syntax:

        `<Name of servers>.<Fully qualified domain name>`

      NOTE: You can use the **Extended** option to make changes to other properties for the Job server. You can also edit the properties later with the Designer.

4. On the **Machine roles** page, select **Job server**.

5. On the **Server functions** page, select **Universal Cloud Interface connector**.

6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

   - For a direct connection to the database:

     a. Select **Process collection | sqlprovider**.

     b. Click the **Connection parameter** entry, then click the **Edit** button.

     c. Enter the connection data for the One Identity Manager database.

   - For a connection to the application server:

     a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.

     b. Click the **Connection parameter** entry, then click the **Edit** button.

     c. Enter the connection data for the application server.

     d. Click the **Authentication data** entry and click the **Edit** button.

     e. Select the authentication module. Depending on the authentication module, other data may be required, for example, user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

7. To configure remote installations, click **Next**.

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

9. On the **Select installation source** page, select the directory with the install files.

10. On the **Select private key file** page, select the file with the private key.

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

11. On the **Service access** page, enter the service's installation data.

    - **Computer**: Name or IP address of the server that the service is installed and started on.

    - **Service account**: User account data for the One Identity Manager Service.

      - To start the service under the **NT AUTHORITY\SYSTEM** account, set the **Local system account** option.

      - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation.

    - **Installation account**: Data for the administrative user account to install the

service.

- To use the current user's account, set the **Current user** option.
- To user another user account, disable the **Current user** option and enter the user account, password and password confirmation.
- To change the install directory, names, display names or description of the One Identity Manager Service, use the other options.

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: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

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 4: 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 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.

Data	Explanation

Table 5: 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.

Data	Explanation
One Identity Manager database connection data	- Database server - Database - SQL Server login and password - Specifies whether integrated 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.
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 the target system to do this. 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 is not possible from the workstation, 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 Synchronization Editor is both:

- Executed in default mode
- Started from the launchpad

If you execute the project wizard in expert mode or directly from Synchronization Editor, additional configuration settings can be made. 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 **Target system type Universal Cloud Interface** entry and click **Start**.

   This starts the Synchronization Editor's project wizard.

3. On the **System access** page, specify how One Identity Manager can access the target system.

   - If access is possible from the workstation on which you started Synchronization Editor, you do not need to make any settings.

   - If access is not possible from the workstation on which you started Synchronization Editor, you can set up a remote connection.

     Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.

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 6: SQL Server database connection data

Data	Description
Server	Database server.
Windows authentication	Specifies whether integrated 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	SQL Server login name.
Password	SQL Server login password.
Database	Database.

- To enter additional information about the database connection, click **Advanced options**.

- Click **Test** to test whether the database is accessible.

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 **Save connection locally** option 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. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

   NOTE: If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again. 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. On the **Restrict target system access** page, you specify how system access should work. You have the following options:

Table 7: Specify target system access

Option	Meaning
Read-only access to target system.	Specifies whether a synchronization workflow is only to be set up for the initial loading of 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 for synchronization in the direction of **One Identity Manager**.
Read/write access to target system. Provisioning available.	Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system.
	The provisioning workflow displays the following characteristics:
	- Synchronization is in the direction of the **Target system**.

Option	Meaning
	• Processing methods are only defined in the synchronization steps for synchronization in the direction of the **Target system**.
	• Synchronization steps are only created for such schema classes whose schema types have write access.

13. On the **Synchronization server** page, select the synchronization server to execute synchronization.

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

    a. Click ▣ to add a new Job server.

    b. Enter a name for the Job server and the full server name conforming to DNS syntax.

    c. Click **OK**.

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

       NOTE: After you save the synchronization project, ensure that this server is set up as a synchronization server.

14. To close the project wizard, click **Finish**.

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

    Table 8: Start up configuration

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 enabled, a consistency check is carried out. If errors occur, a message appears. You can decided whether the synchronization project can remain activated or not.

    Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor's start page, click **Verify project**.

    NOTE: If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually before closing the Synchronization Editor.

NOTE: The connection data for the target system is saved in a variable set and can be modified in the **Configuration | Variables** category in Synchronization Editor.

To configure the content of the synchronization log

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

   NOTE: Some content generates a particularly large volume of log data. The synchronization log should only contain data required for troubleshooting and other analyses.
7. Click **OK**.

To synchronize on a regular basis

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

To start initial synchronization manually

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

NOTE:

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

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

To select user accounts through account definitions

1. Create an account definition.

2. Assign an account definition to the target system.

3. Assign the account definition and manage level to user accounts in **linked** status.

   a. In the Manager, select the **Cloud target systems | <Target system> | User accounts | Linked but not configured | <Target system>** category.

   b. Select the **Assign account definition to linked accounts** task.

Detailed information about this topic

- One Identity Manager Target System Synchronization Reference Guide

Related topics

Start up configuration

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

- Synchronization of the cloud application

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

- Synchronization of pending changes

  If cloud objects are changed in the Cloud Systems Management Module, these changes must first be transferred to the Universal Cloud Interface Module and can then be provisioned to 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 122

Displaying 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. Open the synchronization project in the Synchronization Editor.

2. Select the **Logs** category.

3. Click ▶ in the navigation view toolbar.

   Logs for all completed synchronization runs are displayed in the navigation view.

4. Select a log by double-clicking it.

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

To display a provisioning log.

1. Open the synchronization project in the Synchronization Editor.

2. Select the **Logs** category.

3. Click ⚡ in the navigation view toolbar.

   Logs for all completed provisioning processes are displayed in the navigation view.

4. Select a log by double-clicking 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.

TIP: The logs are also displayed in the Manager under the **<target system> | synchronization log** category.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

- In the Designer, enable the **DPR | Journal | LifeTime** configuration parameter and enter the maximum retention period.

Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization with a Universal Cloud Interface, you can use the 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 objects 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 that 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 for synchronizing 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.

- If another synchronization is started with the same start up configuration, this process is stop and is assigned the **Frozen** execution status. An error message is written to the One Identity Manager Service log file.

  - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start

up configurations different schedules.

- 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.
  - Use the schedule to ensure that the start up configurations are executed in sequence.
  - 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

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). To use One Identity Manager as the master system during synchronization, you also require a workfow with synchronization in the direction of the **Target system**.

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.

   Creates a workflow with **Target system** as its synchronization direction.
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

ONE IDENTITY™

Configuring synchronization of multiple 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.

    - In the wizard, select the Universal Cloud Interface connector and declare the connection parameters. The connection parameters are saved in a special variable set.

        A start up configuration is created that uses the newly created 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 25

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:

ONE IDENTITY™

- 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:
    - Enabling the synchronization project
    - Saving the synchronization project for the first time
    - Compressing a schema

To update a system connection schema

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

    - OR -

    Select the **Configuration | One Identity Manager connection** category.
3. Select the **General** view 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 **Mappings** category.
3. Select a mapping in the navigation view.

    Opens the Mapping Editor. For more detailed information about mappings, see the *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 saves its last execution date as a 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 modified by synchronization are loaded and checked by the next synchronization. This means that the second synchronization after initial synchronization is not significantly faster.

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 **Use revision filter** item from **Revision filtering** menu.

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 **Use revision filter** item from the **Revision filtering** menu.

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.

Outstanding objects

- Cannot be edited in One Identity Manager.

- Are ignored by subsequent synchronization.

- Are ignored by inheritance calculations.

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

Start target system synchronization to do this.

To post-process outstanding objects

1. In the Manager, select **Cloud target systems | Target system synchronization: Universal Cloud Interface**.

All tables assigned to the **Universal Cloud Interface** target system type as synchronization tables are displayed in the navigation view.

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

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

   - The synchronization log has already been deleted.

     - OR -

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

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

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

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

   TIP:

   To display object properties of an outstanding object

   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 9: Methods for handling outstanding objects

Icon	Method	Description
📄✕	Delete	The object is immediately deleted in the One Identity Manager database. Deferred deletion is not taken into account. The **Outstanding** label is removed for the object.
		Indirect memberships cannot be deleted.
📥	Publish	The object is added in the target system. The **Outstanding** label is removed for the object.
		The method triggers the HandleOutstanding event. This runs a target system specific process that triggers the provisioning process for the object.
		Prerequisites:

Icon	Method	Description
		• The table containing the object can be published.
		• The target system connector has write access to the target system.
🖧	Reset	The **Outstanding** label is removed for the object.

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

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

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

To disable bulk processing

- Deactivate ⬚ in the form toolbar.

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 **Connection is read-only** option 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 tables 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 **Cloud Target Systems | Basic configuration data | Target system types** category.
2. Select Universal Cloud Interface in the result list.
3. Select the **Assign synchronization tables** task.

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

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

Accelerating provisioning and single object synchronization

To smooth out spikes in data traffic, handling of processes for provisioning and single object synchronization can be distributed over several Job servers. This will also accelerate these processes.

NOTE: You should not implement load balancing for provisioning or single object synchronization on a permanent basis. Parallel processing of objects might result in dependencies not being resolved because referenced objects from another Job server have not been completely processed.

Once load balancing is not longer required, ensure that the synchronization server executes the provisioning processes and single object synchronization.

To configure load balancing

1. Configure the server and declare it as Job server in One Identity Manager.

   - Assign the **Universal Cloud Interface connector** server function to the Job server.

   All Job servers must access the same cloud target system as the synchronization server for the respective base object.

2. In the Synchronization Editor, assign a custom server function to the base object.

   This server function is used to identify all the Job servers being used for load balancing.

   If there is no custom server function for the base object, create a new one.

   For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

3. In the Manager, assign this server function to all the Job servers that will be processing provisioning and single object synchronization for the base object.

   Only select those Job servers that have the same configuration as the base object's synchronization server.

Once all the processes have been handled, the synchronization server takes over provisioning and single object synchronization again.

To use the synchronization server without load balancing.

- In the Synchronization Editor, remove the server function from the base object.

For detailed information about load balancing, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Editing a server on page 69

Help for the analysis of 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 data store
- 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 **Help | Generate synchronization analysis report** menu item and click **Yes** in the security prompt.

   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.

Disabling synchronization

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

To prevent regular synchronization

1. Open the synchronization project in the Synchronization Editor.
2. 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 synchronization project

1. Open the synchronization project in the Synchronization Editor.
2. Select the **General** view on the start page.
3. Click **Deactivate project**.

Detailed information about this topic

- Creating a synchronization project for initial synchronization of a cloud application on page 16

Basic data for managing a Universal Cloud Interface environment

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. In the Designer, you can find an overview of all configuration parameters in the **Base data | General | Configuration parameters** category.

  For more information, see Configuration parameters for managing cloud target systems on page 128.

- 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 28.

- Account definitions

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

  For more information, see Setting up account definitions on page 34.

- Password policy

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

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

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

For more information, see Password policies for user accounts on page 53.

- 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 64.

- Email notifications about credentials

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

  For more information, see Email notifications about login data on page 65.

- Target system managers

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

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

  For more information, see Target system managers on page 66.

- Server

  Servers must be aware of your server 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 69.

Setting up account definitions

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

The data for the user accounts in the respective target system comes from the basic employee data. The employee must own a central user account. The assignment of the IT operating data to the employee's user account is controlled through the primary assignment of the employee to a location, a department, a cost center, or a business role (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 detailed information about account definitions, 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
- Creating manage levels
- Creating a formatting rule for IT operating data
- Collecting 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. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list. Select the **Change master data** task.

   -OR-

   Click ➕ in the result list.
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 10: Master data for an account definition

Property	Description
Account definition	Account definition name.
User	Table in the One Identity Manager schema that maps user accounts.

Property	Description
account table	
Target system	Target system to which the account definition applies.
Required account definition	Required account definition. 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 field for additional explanation.
Manage level (initial)	Manage level to use by default when you add new user accounts.
Risk index	Value for evaluating the risk of account definition assignments to employees. Enter a value between 0 and 1. This input field is only visible if the **QER	CalculateRiskIndex** configuration parameter 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 also be assigned directly to employees and roles outside of IT Shop.
Only for use in IT Shop	Specifies whether the account definition can only be requested through the IT Shop. The account definition can be ordered by an employee over the Web Portal and distributed using a defined approval process. This means, the account definition cannot be directly assigned to roles outside the IT Shop.
Automatic assignment to employees	Specifies whether the account definition is assigned automatically to all internal employees. The account definition is assigned to every employee not marked as external, on saving. New employees automatically obtain this account definition as soon as they are added. Disable this option to remove automatic assignment of the account definition to all employees. The account definition cannot be reassigned to employees from this point on. Existing account definition assignments remain intact.
Retain	Specifies the account definition assignment to permanently disabled employees.

Property	Description
account definition if permanently disabled	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.

Creating manage levels

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

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

One Identity Manager supplies a default configuration for manage levels:

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

- **Full managed**: User accounts with the **Full managed** manage level inherit defined properties of the assigned employee. When a new user account is created with this manage level and an employee is assigned, the employee's properties are transferred in an initial state. If the employee properties are changed at a later date, the changes are passed onto the user account.

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

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

Specify the effect of temporarily or permanently disabling, deleting, or the security risk of an employee on its user accounts and group memberships for each manage level. For 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. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Assign manage level** task.

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

   - OR -

   Delete the manage levels in **Remove assignments**.

5. Save the changes.

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

To edit a manage level

1. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Manage levels** category.

2. Select the manage level in the result list. Select the **Change master data** task.

- OR -

Click ➕ in the result list.

3. Edit the manage level's master data.

4. Save the changes.

Related topics

-

Master data for manage levels

Enter the following data for a manage level.

Table 11: Master data for manage levels

Property	Description
Manage level	Name of the manage level.
Description	Spare field for additional explanation.
IT operating data overwrites	Specifies whether user account data formatted from IT operating data is automatically updated. Permitted values are: • **Never**: Data is not updated. • **Always**: Data is always updated. • **Only initially**: Data is only determined at the start.
Retain groups if temporarily disabled	Specifies whether user accounts of temporarily 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.
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	Specifies whether user accounts of employees posing a security

Property	Description
security is at risk	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. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Edit IT operating data mapping** task and enter the following data.

Table 12: Mapping rule for IT operating data

Property	Description
Column	User account property for which the value is set. In the menu, you can select the columns that use the `TSB_ITDataFromOrg` script in their template. For detailed information, see the *One Identity Manager Target System Base Module Administration Guide*.

Source	Specifies which roles to use in order to find the user account properties. You have the following options:
	
	• Primary department
	
	• Primary location
	
	• Primary cost center
	
	• Primary business roles
	
	  NOTE: 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 **Always use default value** option.

Default value	Default value of the property for an employee's user account if the value is not determined dynamically from the IT operating data.
Always use default value	Specifies whether user account properties are always filled with the default value. IT operating data is not determined dynamically from a role.
Notify when applying the standard	Specifies whether email notification to a defined mailbox is sent when the default value is used. The **Employee - new user account with default properties created** mail template is used. To change the mail template, adjust the **TargetSystem	CSM	Accounts	MailTemplateDefaultValues** configuration parameter.

4. Save the changes.

Related topics

Collecting IT operating data

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

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

Example

Normally, each employee in department A obtains a default user account in the 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 "Department" property 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 define IT operating data

1. In the Manager, select the role in the **Organizations** or **Business roles** category.

2. Select the **Edit IT operating data** task.

3. Click **Add** and enter the following data.

Table 13: IT operating data

Property	Description
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 field. b. Under **Table**, select the table that maps the target system for select the TSBAccountDef table for an account definition. c. Select the specific target system or account definition under **Effects on**. d. Click **OK**.
Column	User account property for which the value is set. In the menu, you can select the columns that use the TSB_ITDataFromOrg script in their template. For detailed information, see the *One Identity Manager Target System Base Module Administration Guide*.
Value	Concrete value which is assigned to the user account property.

4. Save the changes.

Related topics

- Creating a formatting rule for IT operating data on page 40

Modify IT operating data

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

Prerequisites

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

  - OR -

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

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

To execute the template

1. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Execute templates** task.

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

Old value:	Current value of the object property.
New value:	Value that the object property would have following modification of the IT operating data.
Selection:	Specifies whether the modification shall be adopted for the user account.

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

5. Click **Apply**.

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

Assigning account definitions to employees

Account definitions are assigned to company employees.

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

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

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

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

Prerequisites for indirect assignment of account definitions to employees

- Assignment of employees and account definitions is permitted for role classes (departments, cost centers, locations, or business roles).

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

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. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.
2. Select an account definition in the result list.
3. Select the **Assign organizations** task.
4. Assign organizations in **Add assignments**.

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

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

To remove an assignment

- Select the organization and double-click ⊘.

5. Save the changes.

Related topics

- Assigning an account definition to business roles on page 46
- Assigning account definitions to all employees on page 47
- Assigning account definitions directly to employees on page 47
- Assigning account definitions to system roles on page 48
- Adding account definitions in the IT Shop on page 49

Assigning an account definition to business roles

Installed modules: Business Roles Module

To add account definitions to hierarchical roles

1. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

2. Select an account definition in the result list.

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

4. Assign business roles in **Add assignments**.

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

   To remove an assignment

   - Select the business role and double-click ⊘.

5. Save the changes.

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 45
- Assigning account definitions to all employees on page 47
- Assigning account definitions directly to employees on page 47
- Assigning account definitions to system roles on page 48
- Adding account definitions in the IT Shop on page 49

Assigning account definitions to all employees

To assign an account definition to all employees

1. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

2. Select an account definition in the result list.

3. Select the **Change master data** task.

4. On the **General** tab, enable the **Automatic assignment to employees** option.

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

5. Save the changes.

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

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

Related topics

- Assigning account definitions to departments, cost centers, and locations on page 45
- Assigning an account definition to business roles on page 46
- Assigning account definitions directly to employees on page 47
- Assigning account definitions to system roles on page 48
- Adding account definitions in the IT Shop on page 49

Assigning account definitions directly to employees

To assign an account definition directly to employees

1. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

2. Select an account definition in the result list.

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

4. Assign employees in **Add assignments**.

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

To remove an assignment

- Select the employee and double-click ✅.

5. Save the changes.

Related topics

Assigning account definitions to system roles

Installed modules: System Roles Module

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

To add account definitions to a system role

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

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

   ### To remove an assignment

   - Select the system role and double-click ✅.

5. Save the changes.

Related topics

Adding account definitions in the IT Shop

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

- The account definition must be labeled with the **IT Shop** option.

- The account definition must be assigned to a service item.

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

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

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

To add an account definition to the IT Shop

1. In the Manager, select the **Cloud target systems | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

    - OR -

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

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. Assign the account definitions to the IT Shop shelves in **Add assignments**.

5. Save the changes.

To remove an account definition from individual IT Shop shelves

1. In the Manager, select the **Cloud target systems | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

    - OR -

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

2. Select an account definition in the result list.

3. Select the **Add to IT Shop** task.

4. Remove the account definitions from the IT Shop shelves in **Remove assignments**.

5. Save the changes.

To remove an account definition from all IT Shop shelves

1. In the Manager, select the **Cloud target systems | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

   - OR -

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

2. Select an account definition in the result list.

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

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

5. Click **OK**.

   The account definition is removed from all shelves by 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

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 (**Linked configured** state):

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

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

To assign the account definition to a target system

1. In the Manager, select the target system in the **Cloud target systems** category.

2. Select the **Change master data** task.

3. Select the account definition for user accounts from the **Account definition (initial)** menu.

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 95

Deleting an account definition

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

To delete an account definition

1. Remove automatic assignments of the account definition from all employees.

   a. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

   b. Select an account definition in the result list.

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

   d. Disable the **Automatic assignment to employees** option on the **General** tab.

   e. Save the changes.

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

   a. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

   b. Select an account definition in the result list.

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

   d. Remove employees from **Remove assignments**.

   e. Save the changes.

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

   a. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

   b. Select an account definition in the result list.

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

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

and locations.

    e. Save the changes.

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

    a. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

    b. Select an account definition in the result list.

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

       Remove the business roles in **Remove assignments**.

    d. Save the changes.

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

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

To remove an account definition from all IT Shop shelves

    a. In the Manager, select the **Cloud target systems | Basic configuration data | Account definitions | Account definitions** (non role-based login) category.

       - OR -

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

    b. Select an account definition in the result list.

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

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

    e. Click **OK**.

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

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

    a. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

    b. Select an account definition in the result list.

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

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

    e. Save the changes.

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

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

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

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

   d. Save the changes.

8. Delete the account definition.

   a. In the Manager, select the **Cloud Target Systems | Basic configuration data | Account definitions | Account definitions** category.

   b. Select an account definition in the result list.

   c. Click 🗙 to delete an account definition.

Password policies for user accounts

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

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

Detailed information about this topic

- Predefined password policies on page 53
- Using password policies on page 55
- Editing password policies on page 57
- Custom scripts for password requirements on page 60
- Password exclusion list on page 63
- Checking a password on page 63
- Testing password generation on page 63

Predefined password policies

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

Password for logging in to One Identity Manager

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

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

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

Password policy for forming employees' central passwords

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

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

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

Password policies for user accounts

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

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

NOTE: When you update One Identity Manager version 7.x to One Identity Manager version 8.1.2, the configuration parameter settings for forming passwords are passed on to the target system specific password policies.

The **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.

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

Using password policies

The **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.

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

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

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

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

To reassign a password policy

1. In the Manager, select the **Cloud target systems | Basic configuration data | Password policies** category.
2. Select the password policy in the result list.
3. Select **Assign objects**.

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

Table 14: Assigning a password policy

Property	Description

Apply to	Application scope of the password policy.
	
	To specify an application scope
	
	  a. Click ➜ next to the field.
	
	  b. Select one of the following references under **Table**:
	
	    • The table that contains the base objects of synchronization.
	
	    • To apply the password policy based on the account definition, select the TSBAccountDef table.
	
	    • Select the TSBBehavior table to apply the password policy based on the manage level.
	
	  c. Select the table that contains the base objects under **Apply to**.
	
	    • If you have selected the table containing the base objects of synchronization, next select the specific target system.
	
	    • If you have selected the TSBAccountDef table, next select the specific account definition.
	
	    • If you have selected the TSBBehavior table, next select the specific manage level.
	
	  d. Click **OK**.

Password column	The password column's identifier.
Password policy	The identifier of the password policy to be used.

5. Save the changes.

To change a password policy's assignment

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

Editing password policies

To edit a password policy

1. In the Manager, select the **Cloud target systems | Basic configuration data | Password policies** category.

2. Select the password policy in the result list and select **Change master data**.

   - OR -

   Click 🔲 in the result list.

3. Edit the password policy's master data.

4. Save the changes.

Detailed information about this topic

- General master data for password policies on page 57
- Policy settings on page 58
- Character classes for passwords on page 59
- Custom scripts for password requirements on page 60

General master data for password policies

Enter the following master data for a password policy.

Table 15: Master data for a password policy

Property	Meaning
Display name	Password policy name. Translate the given text using the 🌐 button.
Description	Spare field 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 **One Identity Manager password policy** is marked as the default policy. This password policy is applied if no other password policy can be found for employees, user accounts, or system users.

Policy settings

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

Table 16: Policy settings

Property	Meaning
Initial password	Initial password for newly created user accounts. The initial password is used if a password is not entered when you create a user account or if a random password is not generated.
Password confirmation	Reconfirm password.
Minimum Length	Minimum length of the password. Specify the number of characters a password must have.
Max. length	Maximum length of the password. Specify the number of characters a password can have. The maximum permitted value is **256**.
Max. errors	Maximum number of errors. Set the number of invalid passwords. Only taken into account when logging in to One Identity Manager.
	This data is only taken into account if the One Identity Manager login was through a system user or employee based authentication module. If a user has reached the number of maximum failed logins, the employee or system user can no longer log in to One Identity Manager.
	You can reset the passwords of employees and system users who have been blocked in Password Reset Portal. For more detailed information, see the *One Identity Manager Web Portal User Guide*.
Validity period	Maximum age of the password. Enter the length of time a password can be used before it expires.
Password history	Enter the number of passwords to be saved. If, for example, a value of **5** is entered, the user's last five passwords are stored.
Minimum password strength	Specifies how secure the password must be. The higher the password strength, the more secure it is. The value **0** means that the password strength is not tested. The values **1**, **2**, **3** and **4** specify the required complexity of the password. The value **1** represents the lowest requirements in terms of password strength. The value **4** requires the highest level of complexity.
Name properties denied	Specifies whether name properties are permitted or not

Property	Meaning
	permitted in the password. If this option is enabled, name properties are not permitted in passwords. The values of the columns for which the **Contains name properties for password check** option is set are taken into account. In the Designer, adjust this option in the column definition. For more detailed information, see the *One Identity Manager Configuration Guide*.

Character classes for passwords

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

Table 17: Character classes for passwords

Property	Meaning
Min. number letters	Specifies the minimum number of alphabetical characters the password must contain.
Min. number lowercase	Specifies the minimum number of lowercase letters the password must contain.
Min. number uppercase	Specifies the minimum number of uppercase letters the password must contain.
Min. number digits	Specifies the minimum number of digits the password must contain.
Min. number special characters	Specifies the minimum number of special characters the password must contain.
Permitted special characters	List of permitted characters.
Max. identical characters in total	Maximum number of identical characters that can be present in the password in total.
Max. identical	Maximum number of identical character that can be repeated after each other.

Property	Meaning
characters in succession	
Denied special characters	List of characters, which are not permitted.
Do not generate lowercase letters	Specifies whether or not a generated password can contain lowercase letters. This setting is only applies when passwords are generated.
Do not generate uppercase letters	Specifies whether or not a generated password can contain uppercase letters. This setting is only applies when passwords are generated.
Do not generate digits	Specifies whether or not a generated password can contain digits. This setting is only applies when passwords are generated.
Do not generate special characters	Specifies whether or not a generated password can contain special characters. If this option is set, only letters, numbers, and spaces are allowed in passwords. This setting is only applies when passwords are generated.

Custom scripts for password requirements

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

Detailed information about this topic

Script for checking passwords

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

Syntax of check scripts

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

With parameters:

policy = password policy object

spwd = password to check

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

Example of a script that checks a password

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

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

To use a custom script for checking a password

1. In the Designer, create your script in the **Script Library** category.

2. Edit the password policy.

   a. In the Manager, select the **Cloud target systems | Basic configuration data | Password policies** category.

   b. Enter the name of the script to be used to check a password in the **Check script** field on the **Scripts** tab.

   c. Save the changes.

Related topics

- Script for generating a password on page 62

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 `Entity` property of the `PasswordPolicy` class.

Example for a script to generate a password

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

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

    Dim pwd = spwd.ToInsecureArray()

    ' replace invalid characters at first position

    If pwd.Length>0

        If pwd(0)="?" Or pwd(0)="!"

            spwd.SetAt(0, CChar("_"))

        End If

    End If

End Sub
```

To use a custom script for generating a password

1. In the Designer, create your script in the **Script Library** category.

2. Edit the password policy.

   a. In the Manager, select the **Cloud target systems | Basic configuration data | Password policies** category.

   b. Enter the name of the script to be used to generate a password in the **Generating script** input field on the **Scripts** tab.

   c. Save the changes.

Related topics

- Script for checking passwords on page 60

Password exclusion list

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

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

To add a term to the restricted list

1. In the Designer, select the **Base Data | Security settings | Restricted passwords** category.

2. Create a new entry with the **Object | New** menu item and enter the term to exclude to the list.

3. Save the changes.

Checking a password

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

To check if a password conforms to the password policy

1. In the Manager, select the **Cloud target systems | Basic configuration data | Password policies** category.

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 password generation

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

To generate a password that conforms to the password policy

1. In the Manager, select the **Cloud target systems | Basic configuration data | Password policies** category.

2. Select the **Test** tab.

3. Click **Generate**.

   This generates and displays a password.

Initial password for new user accounts

Table 18: Configuration parameters for formatting initial passwords for user accounts

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

- Create user accounts manually and enter a password in their master data.
- Assign a randomly generated initial password to enter when you create user accounts.
  - In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword** configuration parameter.
  - Apply target system specific password policies and define the character sets that the password must contain.
  - Specify which employee will receive the initial password by email.
- User the employee's central password. The employee's central password is mapped to the user account password. For detailed information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

Email notifications about login data

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

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

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

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

To send initial login data by email

1. In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword** configuration parameter.

2. In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword | SendTo** configuration parameter and enter the recipient of the notification as a value.

3. In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName** configuration parameter.

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

4. In the Designer, set the **TargetSystem | CSM | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword** configuration parameter.

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

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

Target system managers

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

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

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

Implementing application roles for target system managers

1. The One Identity Manager administrator assigns employees to be target system managers.

2. These target system managers add employees to the default application role for target system managers.

Target system managers with the default application role are authorized to edit all the cloud target systems in One Identity Manager.

3. Target system managers can authorize other employees within their area of responsibility as target system managers and if necessary, create additional child application roles and assign these to individual cloud target systems.

Table 19: Default application roles for target system managers

User	Tasks
Target system managers	Target system managers must be assigned to the **Target systems | Cloud target systems** application role or a child application role.

Users with this application role:

- Assume administrative tasks for the target system.
- Create, change, or delete target system objects, like user accounts or groups.
- Edit password policies for the target system.
- Prepare groups for adding to the IT Shop.
- Can add employees, who have an other identity than the **Primary identity**.
- Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager.
- Edit the synchronization's target system types and outstanding objects.
- Authorize other employees within their area of responsibility as target system managers and create child application roles if required.

To initially specify employees to be target system administrators

1. Log in to Manager as One Identity Manager administrator (**Base role \| Administrators** application role)

2. Select the **One Identity Manager Administration \| Target systems \| Administrators** category.

3. Select the **Assign employees** task.

4. Assign the employee you want and save the changes.

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

1. Log in to Manager as target system administrator (**Target systems \| Administrators** application role).

2. Select the **One Identity Manager Administration \| Target systems \| Cloud**

target systems category.

3. Select the **Assign employees** task.

4. Assign the employees you want and save the changes.

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

1. Log in to Manager as target system manager.

2. Select the application role in the **Custom Target Systems | Basic configuration data | Target system managers** category.

3. Select the **Assign employees** task.

4. Assign the employees you want and save the changes.

To specify target system managers for individual cloud target systems

1. Log in to the Manager as target system manager.

2. Select the **Cloud Target Systems | Basic configuration data | Cloud target systems** category.

3. Select the target system in the result list.

4. Select the **Change master data** task.

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

   - OR -

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

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

   b. Click **OK** to add the new application role.

6. Save the changes.

7. Assign employees to this application role who are permitted to edit the target system in One Identity Manager.

Related topics

- One Identity Manager users for managing cloud target systems on page 8
- General master data for a cloud target system on page 74
- Container structures in a cloud target system on page 79

Editing a server

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

- In the Designer, create an entry for the Job server in the **Base Data | Installation | Job server** category. For detailed information, see *One Identity Manager Configuration Guide*.

- In the Manager, select an entry for the Job server in the **Could target systems | Basic configuration data | Server** category and edit the Job server master data category.

    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 described in the *One Identity Manager Installation Guide*.

To edit a Job server and its functions

1. In the Manager, select the **Cloud target systems | Basic configuration data | Server** category.
2. Select the Job server entry in the result list.
3. Select the **Change master data** task.
4. Edit the Job server's master data.
5. Select the **Assign server functions** task and specify server functionality.
6. Save the changes.

Detailed information about this topic

- Master data for a Job server on page 69
- Specifying server functions on page 72

Related topics

- Setting up the synchronization server on page 13

Master data for a Job server

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

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

Table 20: 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	Language of the server.
Server is cluster	Specifies whether the server maps a cluster.
Server belongs to cluster	Cluster to which the server belongs. NOTE: The **Server is cluster** and **Server belongs to cluster** properties are mutually exclusive.
IP address (IPv6)	Internet protocol version 6 (IPv6) server address.
IP address (IPv4)	Internet protocol version 4 (IPv4) server address.
Copy process (source server)	Permitted copying methods that can be used when this server is the source of a copy action. At present, only copy methods that support the `Robocopy` and `rsync` programs are supported. If no method is given, the One Identity Manager Service determines the operating system of the server during runtime. Replication is then performed with the `Robocopy` program between servers with a Windows operating system or with the `rsync` program between servers with a Linux operating system. If the operating systems of the source and destination servers differ, it is important that the right copy method is applied for successful replication. A copy method is chosen that supports both servers.
Copy process (target server)	Permitted copying methods that can be used when this server is the destination of a copy action.
Coding	Character set coding that is used to write files to the server.
Parent Job server	Name of the parent Job server.

ONE IDENTITY™

Property	Meaning
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 the 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 this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time.
	The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks.
	You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more detailed information, see the *One Identity Manager Process Monitoring and Troubleshooting Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating.
	NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently being executed.
Last fetch time	Last time the process was collected.
Last	The time of the last check for loaded process steps with a dispatch value that

Property	Meaning
timeout check	exceeds the one in the **Common | Jobservice | LoadedJobsTimeOut** configuration parameter.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related topics

Specifying server functions

NOTE: All editing options are also available in the Designer under **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 21: 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 One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.
SQL processing server	The server can execute SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	The server can process CSV files using the `ScriptComponent` process component.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
SMTP host	Server from which One Identity Manager Service sends email notifications. Prerequisite for sending mails using One Identity Manager Service is SMTP host configuration.

Server function	Remark
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 69

Cloud target systems

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

NOTE: The Synchronization Editor sets up the cloud target systems in the One Identity Manager database.

To edit a cloud system's master data

1. Select the **Cloud Target Systems | Basic configuration data | Cloud target systems** category.

2. Select the target system in the result list. Select the **Change master data** task.

3. Edit the target system type master data.

4. Save the changes.

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

Detailed information about this topic

- General master data for a cloud target system on page 74
- Specifying categories for inheriting groups on page 77
- Alternative column names on page 77

General master data for a cloud target system

Enter the following master data for a cloud target system.

Table 22: Cloud target system master data

Property	Description
Cloud target	Name of the target system.

Property	Description
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 (**Linked configured** state). The account definition's default manage level is applied. User accounts are only linked to the employee (**Linked** state) if no account definition is given. This is the case on initial synchronization, for example.
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	Type of synchronization through which the data is synchronized between the target system and One Identity Manager. You can no longer change the synchronization type once objects for this target system are present in One Identity Manager. If you create a cloud target system with the Synchronization Editor, **One Identity Manager** is used.

Property	Description

Table 23: Permitted values

Value	Synchronization by	Provisioned by
One Identity Manager	Universal Cloud Interface connector	Universal Cloud Interface connector
No synchronization	none	none

NOTE: If you select **No synchronization**, you can define custom processes to exchange data between One Identity Manager and the target system.

Property	Description
Description	Spare field for additional explanation.
Manual provisioning	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 and • between the modules Universal Cloud Interface and Cloud Systems Management is kept consistent!
User account deletion not permitted	Specifies whether user accounts in the cloud target system can be deleted. If this option is set, user account can only be disabled.

Related topics

- Automatic assignment of employees to user accounts on page 95
- Target system managers on page 66

ONE IDENTITY™

Specifying categories for inheriting groups

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

To define a category

1. In the Manager, select the target system in the **Cloud target systems** category.

2. Select the **Change master data** task.

3. Switch to the **Mapping rule category** tab.

4. Extend the relevant roots of the user account table or group table.

5. To enable the category, double-click ⊗.

6. Enter a category name of your choice for user accounts and groups and in the login language used.

7. Save the changes.

Detailed information about this topic

- Group inheritance based on categories on page 114

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 **Cloud Target Systems | Basic configuration data | Cloud target systems** category.

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

3. Switch to the **Alternative column names** tab.

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

   All the columns in this table are listed with their default column names.

5. Enter any name in the login language in use.

6. Save the changes.

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 in 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 **Cloud Target Systems | Basic configuration data | Cloud target systems** category.

2. Select the target system in the result list. Select the **Change master data** task.

3. Select the **Edit synchronization project...** task.

Related topics

- Customizing the synchronization configuration on page 24

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

   - OR -

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

Enter the following master data for a container.

Table 24: 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 field for additional explanation.
Account manager	Manager responsible for the container. ***To specify an account manager***

Property	Description
	1. Click ➔ next to the field.
	2. In the **Table** menu, select the table that maps the account manager.
	3. In the **Account manager** menu, select the 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 66

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

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

- Employees can automatically obtain their account definitions using user account resources. If an employee does not yet have a user account 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 and subsequent process handling.

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

- When user accounts are inserted, they can be automatically assigned to an existing employee or a new employee can be created if necessary. In the process, the employee master data is created on the basis of existing user account master data. This mechanism can be implemented if a new user account is created manually or by synchronization. However, this is not the One Identity Manager default method. Define criteria for finding employees for automatic employee assignment.

- Employees and user accounts can be entered manually and assigned to each other.

Related topics

- Entering user account master data on page 86
- Setting up account definitions on page 34
- Automatic assignment of employees to user accounts on page 95

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, service accounts, or privileged user accounts can be mapped in One Identity Manager.

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

- Identity

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

Table 25: Identities of user accounts

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

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

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

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

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

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

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

- Privileged user account

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

Default user accounts

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

To create default user accounts through account definitions

1. Create an account definition and assign the **Unmanaged** and **Full managed** manage levels.

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

3. Create a formatting rule for IT operating data.

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

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

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

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

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

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

5. Assign the account definition to employees.

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

Administrative user accounts

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

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

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

You can label administrative user accounts as a **Personalized administrator identity** or as a **Shared identity**. Proceed as follows to provide the employees who use this user account with the required permissions.

- Personalized admin identity

   1. Use the `UID_Person` column to link the user account with an employee.

      Use an employee with the same identity or create a new employee.

2. Assign this employee to hierarchical roles.

- Shared identity
    1. Assign all employees with usage authorization to the user account.
    2. Link the user account to a dummy employee using the `UID_Person` column.

       Use an employee with the same identity or create a new employee.
    3. Assign this dummy employee to hierarchical roles.

    The dummy employee provides the user account with its permissions.

Privileged user accounts

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

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

To create privileged users through account definitions

1. Create an account definition. Create a new manage level for privileged user accounts and assign this manage level to the account definition.

2. If you want to prevent the properties for privileged user accounts from being overwritten, set the **IT operating data overwrites** property for the manage level to **Only initially**. In this case, the properties are populated just once when the user accounts is created.

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

4. Create a formatting rule for IT operating data.

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

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

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

   - You can also specify a mapping rule for the `IdentityType` column. The column owns different permitted values that represent user accounts.

   - To prevent privileged user accounts from inheriting the entitlements of the default user, define a mapping rule for the `IsGroupAccount` column with a default value of **0** and set the **Always use default value** option.

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

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

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

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

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

Entering user account master data

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

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

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

To create a user account

1. In the Manager, select the **Cloud Target Systems | <target system> | User accounts** category.

2. Click ![icon] in the result list.

3. On the master data form, edit the master data for the user account.

4. Save the changes.

To edit master data for a user account

1. In the Manager, select the **Cloud Target Systems | <target system> | User accounts** category.

2. Select the user account in the result list and run the **Change master data** task.

3. Edit the user account's resource data.

4. Save the changes.

To manually assign or create a user account for an employee

1. In the Manager, select the **Employees | Employees** category.

2. Select the employee in the result list and run the **Assign cloud user accounts** task.

3. Assign a user account.

4. Save the changes.

Detailed information about this topic

- Additional master data for a user account on page 87
- User account login data on page 90
- Identification details on page 91
- Contact data on page 92
- User-defined master data on page 92

Related topics

- Deleting user accounts on page 100

Additional master data for a user account

Table 26: Configuration parameters for risk assessment of user accounts

Configuration parameter	Effect when set
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 enabled, values for the risk index can be entered and calculated.

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

Table 27: User account properties

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

Property	Description
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. One Identity Manager finds the IT operating data of the assigned employee and enters it in the corresponding fields in the user account.
	NOTE: The account definition cannot be changed once the user account has been saved.
Manage level	Manage level of the user account. Select a manage level from the menu. You can only specify the manage level can if you have also entered an account definition. All manage levels of the selected account definition are available in the menu.
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 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	User account's primary group.

Property	Description
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 a leaving date is specified for an employee, this date is used as the account expiration date depending on the manage level. Any existing account expiry date is overwritten in this case. NOTE: If the employee's leaving date is deleted at a later point in time, the user account expiration date remains intact!
Resource type	Type of the resource, for example, user.
Risk index (calculated)	Maximum risk index value of all assigned groups. The property is only visible if the **QER	CalculateRiskIndex** configuration parameter is set. For more detailed information, see the *One Identity Manager Risk Assessment Administration Guide*.
Category	Categories for the inheritance of groups by the user account. Groups can be selectively inherited by user accounts. To do this, groups and user accounts or contacts are divided into categories. Select one or more categories from the menu.
Description	Spare field 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 Permitted values are: • **Primary identity**: Employee's default user account. • **Organizational identity**: Secondary user account used for different roles in the organization, for example for subcontracts with other functional areas. • **Personalized administrator identity**: User account with administrative entitlements, used by one employee. • **Sponsored identity**: User account that is used for training

Property	Description
	purposes, for example. • **Shared identity**: User account with administrative entitlements, used by several employees. Assign all employees show use the user account. • **Service identity**: Service account.
Privileged user account	Specifies whether this is a privileged user account.
Groups can be inherited	Specifies whether the user account can inherit groups through the employee. If this option is set, the user account inherits groups through hierarchical roles or IT Shop requests. • If you add an employee with a user account to a department, for example, and you have assigned groups to this department, the user account inherits these groups. • If an employee has requested group membership in the IT Shop and the request is granted approval, the employee's user account only inherits the group if the option is set.
User account is disabled	Specifies whether the user account is locked. If a user account is not required for a period of time, you can temporarily disable the user account by using the <User account is deactivated> option.

Related topics

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 28: User account login data

Property	Description
Password/Password confirmation	Password for the user account. The employee's central password can be mapped to the user account password. For detailed information about an employee's central password, see *One Identity Manager Identity Management Base Module Administration Guide*.

Property	Description
	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 for user accounts on page 53

Identification details

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

Table 29: Identification data for a user account

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

Property	Description

To specify an account manager

1. Click ➜ next to the field.

2. In the **Table** menu, select the table that maps the account manager.

3. In the **Account manager** menu, select the manager.

4. Click **OK**.

Contact data

You can find the information about the employee contact information used by this user account on the **Contact** tab.

Table 30: 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 31: Customized master data for a user account

Property	Description
Spare field 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.

Property	Description
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 run the following tasks.

Overview of the user account

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

To obtain an overview of a user account

1. Select the **Cloud Target Systems | <target system> | User accounts** category.

2. Select the user account in the result list.

3. Select the **User account overview** task.

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, such as 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. In the Manager, select the **Cloud Target Systems | <target system> | User accounts** category.

2. Select the user account in the result list.

3. Select the **Assign groups** category.

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

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

To remove an assignment

- Select the group and double-click ⊘.

5. Save the changes.

NOTE: The primary group of a user account is already assigned and is marked as **Does not apply yet**. Edit the user account's master data to change its primary group.

Related topics

- Assigning groups to user accounts on page 105

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 **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** category.
5. Save the changes.

Assigning extended properties

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

To specify extended properties for a user account

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

   - OR -

   Remove 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 32: 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 are listed 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 on the basis of existing user account 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 **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 that the manage level to be used is entered as the default manage 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 a synchronization, employees are automatically created for the user accounts in the default installation. If an account definition for the target system is not yet known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

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

To select user accounts through account definitions

1. Create an account definition.

2. Assign an account definition to the target system.

3. Assign the account definition and manage level to user accounts in **linked** status.

   a. In the Manager, select the **Cloud target systems | <Target system> | User accounts | Linked but not configured | <Target system>** category.

   b. Select the **Assign account definition to linked accounts** task.

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

Related topics

Editing search criteria for automatic employee assignment

The criteria for employee assignment are defined for the target system. In this case, you specify which user account properties must match the employee's properties such that the employee can be assigned to the user account. You can limit search criteria further by using format definitions. The search criterion is written in XML notation to the **Search criteria for automatic employee assignment** column (`AccountToPersonMatchingRule`) in the `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 **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 **Cloud Target Systems | Basic configuration data | Cloud target systems** category.
2. Select the target system in the result list.
3. Select the **Define search criteria for employee assignment** task.
4. Specify which user account properties must match with which employee so that the employee is linked to the user account.

Table 33: Example of search criteria for user accounts

Apply to	Column for employee	Column for user account
Cloud user accounts	FirstName AND LastName	FirstName AND LastName

5. Save the changes.

Direct assignment of employees to user accounts based on a suggestion list

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

Table 34: 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. Check the **Selection** box of all the user accounts to which you want to assign the suggested employees. Multi-select is possible.

   b. Click **Assign selected.**

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

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

   – OR –

2. Click **No employee assignment**.

   a. Click the **Select employee** option of the user account to which you want to assign an employee. Select an employee from the menu.

b. Check the **Selection** box of all the user accounts to which you want to assign the selected employees. Multi-select is possible.

c. Click **Assign selected**.

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

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

To remove assignments

1. Click **Assigned user accounts**.

    a. Click the **Selection** box of all user accounts you want to delete the employee assignment from. Multi-select is possible.

    b. Click **Remove selected**.

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

    The assigned employees are removed from the selected user accounts.

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

Related topics

- Automatic assignment of employees to user accounts on page 95

Locking and unlocking user accounts

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

Scenario:

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

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

Scenario:

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

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

- If the configuration parameter is set, the employee's user accounts are disabled if the employee is permanently or temporarily disabled.

- If the configuration parameter is not set, the employee's properties do not have any effect on the associated user accounts.

To disable the user account when the configuration parameter is disabled.

1. In the Manager, select the **Cloud Target Systems | <target system> | User accounts** category.

2. Select the user account in the result list.

3. Select the **Change master data** task.

4. Enable the **Account is disabled** option on the **General** tab.

5. Save the changes.

Scenario:

- User accounts not linked to employees.

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

1. In the Manager, select the **Cloud Target Systems | <target system> | User accounts** category.

2. Select the user account in the result list.

3. Select the **Change master data** task.

4. Enable the **Account is disabled** option 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
- Creating manage levels on page 37

Deleting user accounts

You can delete a user account from the result list or the menu base. After the security prompt 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 deferred deletion has expired. In the Designer, you can set an alternative delay on the CMSUser table.

To delete a user account

1. Select the **Cloud Target Systems | <target system> | User accounts** category.

2. Select the user account in the result list.

3. Click in the result list.

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

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 **Cloud Target Systems | Basic configuration data | Cloud target systems** category.

2. Select the target system in the result list. Select the **Change master data** task.

3. Set the **User account deletion not permitted** option.

4. Save the changes.

Detailed information about this topic

- Provisioning object changes on page 122
- General master data for a cloud target system on page 74
- Locking and unlocking user accounts on page 99

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. In the Manager, select the **Cloud Target Systems | <target system> | Groups** category.

2. Select the group in the result list and run the **Change master data** task.

3. On the master data form, edit the master data for the group.

4. Save the changes.

Detailed information about this topic

Entering master data for a group

Table 35: Configuration parameters for risk assessment of user accounts

Configuration parameter	Effect when set
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 enabled, values for the risk index can be entered and calculated.

Enter the following master data for a group.

Table 36: Entering master data for a group

Property	Description
Name	Name of the group.
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 field. 2. In the **Table** menu, select the table that maps the account manager. 3. In the **Account manager** menu, select the manager. 4. Click **OK**.
IT Shop	Specifies whether the group can be requested through the IT Shop. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. The group can still be assigned directly to hierarchical roles. 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. If this option is set, the group can be requested by the employees through the Web Portal and distributed with a defined approval process. Direct assignment of the group to hierarchical roles or user accounts is no permitted.
Service item	Service item data for requesting the group through the IT Shop.
Risk index	Value for evaluating the risk of assigning the group to user accounts. Enter a value between 0 and 1. This input field is only visible if the **QER | CalculateRiskIndex** configuration parameter is activated. For more detailed information, see the One Identity Manager Risk Assessment Administration Guide.

Property	Description
Category	Categories for group inheritance. Groups can be selectively inherited by user accounts. To do this, groups, and user accounts are divided into categories. Select one or more categories from the menu. For more detailed information, see the One Identity Manager Target System Base Module Administration Guide.
Description	Spare field 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

User-defined master data for a group

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

Table 37: User-defined master data for a group

Property	Description
Spare field 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 (departments, cost centers, locations, or business roles).
- Cloud user accounts are marked with the **Groups can be inherited** option.
- Cloud user accounts and cloud groups belong to the same target system.

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

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

Detailed information about this topic

- Assigning groups to departments, cost centers, and locations on page 105
- Assigning groups to business roles on page 106
- Assigning user accounts directly to a group on page 107
- Adding groups to system roles on page 108
- Adding groups to the IT Shop on page 109

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. In the Manager, select the **Cloud Target Systems | <target system> | Groups** category.

2. Select the group in the result list.

3. Select the **Assign organizations** task.

4. Assign organizations in **Add assignments**.

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

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

   To remove an assignment

   - Select the organization and double-click ⊘.

5. Save the changes.

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

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

   - OR -

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

   - OR -

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

2. Select the department, cost center, or location in the result list.

3. Select the **Assign cloud groups** task.

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

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

   To remove an assignment

   - Select the group and double-click ⊘.

5. Save the changes.

Related topics

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. In the Manager, select the **Cloud Target Systems | <target system> | Groups** category.

2. Select the group in the result list.

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

4. Assign business roles in **Add assignments**.

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

   #### To remove an assignment

   - Select the business role and double-click ⊘.

5. Save the changes.

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

1. In the Manager, select the **Business roles | <role class>** category.

2. Select the business role in the result list.

3. Select the **Assign cloud groups** task.

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

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

   #### To remove an assignment

   - Select the group and double-click ⊘.

5. Save the changes.

Related topics

Assigning user accounts directly to a group

Groups can be assigned directly or indirectly to user accounts. Indirect assignment is done by allocating the employee and groups into company structures such as 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. In the Manager, select the **Cloud Target Systems | <target system> | Groups** category.

2. Select the group in the result list.

3. Select the **Assign user accounts** task.

4. Assign user accounts in **Add assignments**.

   > TIP: In **Remove assignments**, you can remove the assignment of user accounts.
   >
   > ### To remove an assignment
   >
   > - Select the user account and double-click ⊘.

5. Save the changes.

Related topics

- Assigning groups directly to user accounts on page 93
- Assigning groups to departments, cost centers, and locations on page 105
- Assigning groups to business roles on page 106
- Adding groups to system roles on page 108
- Adding groups to the IT Shop on page 109

Adding groups to system roles

Installed modules: System Roles Module

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

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

To assign a group to system roles

1. In the Manager, select the **Cloud Target Systems | <target system> | Groups** category.

2. Select the group in the result list.

3. Select the **Assign system roles** task.

4. Assign system roles in **Add assignments**.

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

To remove an assignment

- Select the system role and double-click ⊘.

5. Save the changes.

Related topics

Adding groups to the IT Shop

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

- the group must be marked with the **IT Shop** option.

- the group must be assigned a service item.

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

- If you only want it to be possible for the group to be assigned to employees through IT Shop requests, the group must also be labeled with the **Use only in IT Shop** option. Direct assignment to hierarchical roles or user accounts is no longer permitted.

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

To add a group to IT Shop.

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

    - OR -

    In the Manager, select the **Entitlements | Cloud groups** (role-based login) category.

2. In the result list, select the group.

3. Select the **Add to IT Shop** task.

4. In **Add assignments**, assign the group to the IT Shop shelves.

5. Save the changes.

To remove a group from individual shelves of the IT Shop

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

   - OR -

   In the Manager, select the **Entitlements | Cloud groups** (role-based login) category.

2. In the result list, select the group.

3. Select the **Add to IT Shop** task.

4. In **Remove assignments**, remove the group from the IT Shop shelves.

5. Save the changes.

To remove a group from all shelves of the IT Shop

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

   - OR -

   In the Manager, select the **Entitlements | Cloud groups** (role-based login) category.

2. In the result list, select the group.

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

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

5. Click **OK**.

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

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

Related topics

-
-
-
-
-

Additional tasks for managing groups

After you have entered the master data, 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 **Cloud Target Systems | <target system> | Groups** category.

2. Select the group in the result list.

3. Select the **Group overview** task.

Adding groups to groups

Use this task to add a group to another group.

To assign groups directly to a group

1. In the Manager, select the **Cloud Target Systems | <target system> | Groups** category.

2. Select the group in the result list.

3. Select the **Assign groups** category.

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

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

   To remove an assignment

   - Select the group and double-click ⊘.

5. Save the changes.

Effectiveness of group memberships

Table 38: Configuration parameters for conditional inheritance

Configuration parameter	Effect when set
QER | Structures | Inherit | GroupExclusion	Preprocessor relevant configuration parameter for controlling effectiveness of group memberships. If the parameter is set, memberships can be reduced on the basis of exclusion definitions. Changes to this parameter require the database to be recompiled.

When groups are assigned to user accounts an employee may obtain two or more groups, which are not permitted in this combination. To prevent this, you can declare mutually

exclusive groups. To do this, you specify which of the two groups should apply to the user accounts if both are assigned.

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

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

The effectiveness of the assignments is mapped in the CSMUserInGroup and CSMBaseTreeHasGroup tables by the XIsInEffect column.

Example of the effect of group memberships

- Group A is assigned through the "Marketing" department, group B through "Finance", and group C through the "Control group" business role.

Clara Harris has a user account in this target system. She primarily belongs to the "marketing" department. The "Control group" business role and the "Finance" department 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 39: Specifying excluded groups (CSMGroupExclusion table)

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

Table 40: Effective assignments

Employee	Member in Role	Effective Group
Ben King	Marketing	Group A

ONE IDENTITY™

Employee	Member in Role	Effective Group
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 "control group" business role 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 41: 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 **QER | Structures | Inherite | GroupExclusion** configuration parameter is set.
- Mutually exclusive groups belong to the same cloud target system.

To exclude a group

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

   - OR -

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

Group inheritance based on categories

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

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 position 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 42: Category examples

Category position	Categories for user accounts	Categories for groups
1	Default user	Default entitlements
2	System users	System user entitlements
3	System administrator	System administrator entitlements

Figure 2: Example of inheriting through categories.
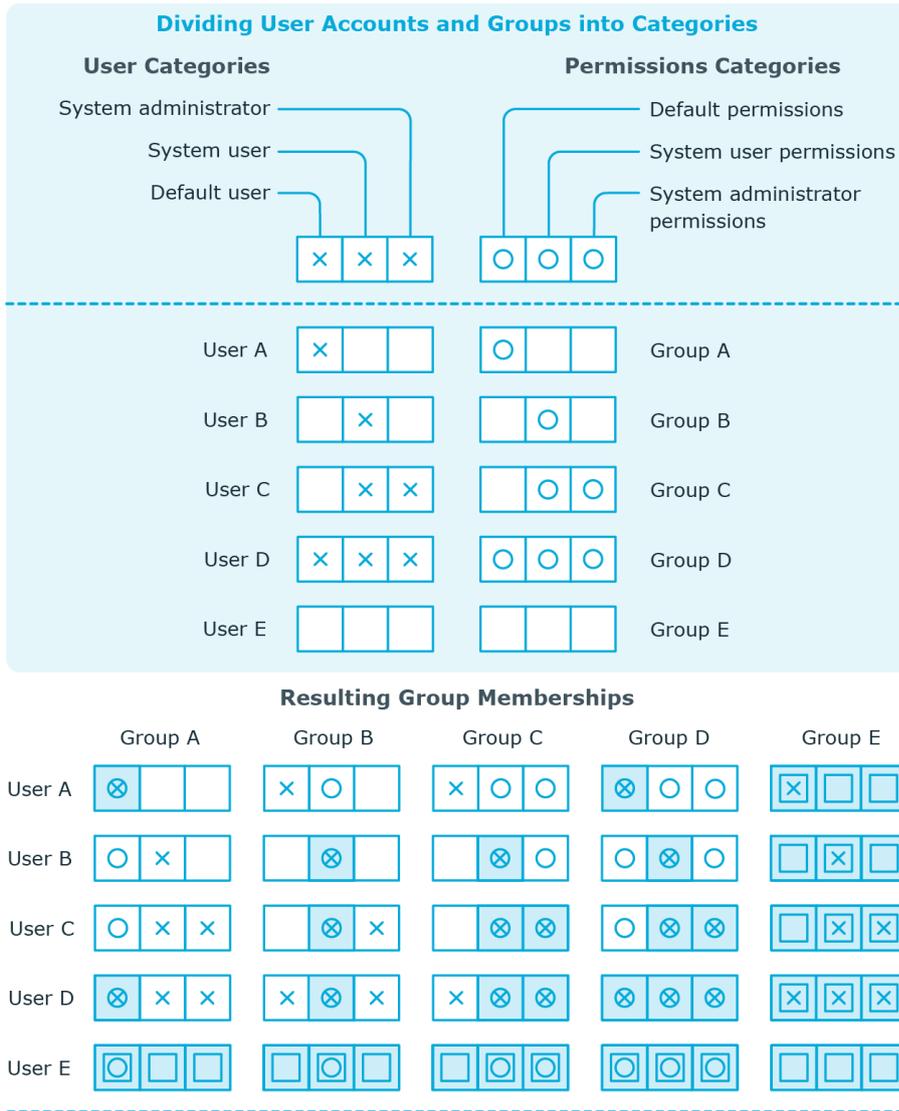
To use inheritance through categories

- 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 77
- Additional master data for a user account on page 87
- Entering master data for a group on page 102

Assigning permissions controls

Use this task to assign permissions controls to groups.

To assign permissions controls to a group

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

    - OR -

    In **Remove assignments** double-click on the permissions controls for which you want to delete the assignment.
5. Save the changes.

Related topics

- Cloud permissions controls on page 118

Assigning extended properties

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

To specify extended properties for a group

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

    - OR -

    Remove extended properties in **Remove assignments** category..
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 **Cloud Target Systems | <target system> | Groups** category.
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 122

Cloud permissions controls

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

To edit permissions controls

1. Select the **Cloud Target Systems | <target system> | Permissions controls** category.

2. Select the permissions control in the result list. Select the **Change master data** task.

   - OR -

   Click in the result list.

3. Edit the permissions controls' master data.

4. Save the changes.

Detailed information about this topic

- General master data for permissions controls on page 118
- User-defined master data for permissions controls on page 119

General master data for permissions controls

Enter the following master data for a permissions control.

Table 43: 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 field for additional explanation.

User-defined master data for permissions controls

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

Table 44: User-defined master data for permissions controls

Property	Description
Spare field 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 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 **Cloud Target Systems | <target system> | Permissions controls** category.

2. Select the permissions control in the result list.

3. Select the **Permissions control overview** task.

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 **Cloud Target Systems | <target system> | Permissions controls** category.

2. Select the permissions control in the result list.

3. Select the **Assign user accounts** task.

4. Assign user accounts in **Add assignments**.

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

   ### To remove an assignment

   - Select the user account and double-click ✅.

5. Save the changes.

Assigning permissions controls to groups

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

To assign permissions controls to groups

1. Select the **Cloud Target Systems | <target system> | Permissions controls**.

2. Select the permissions control in the result list.

3. Select **Assign groups** category.

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

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

   ### To remove an assignment

   - Select the group and double-click ✅.

5. Save the changes.

Deleting permissions controls

To delete a permissions control

1. Select the **Cloud Target Systems | <target system> | Permissions controls** category.

2. Select the permissions control in the result list.

3. Click ![icon] 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 122

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

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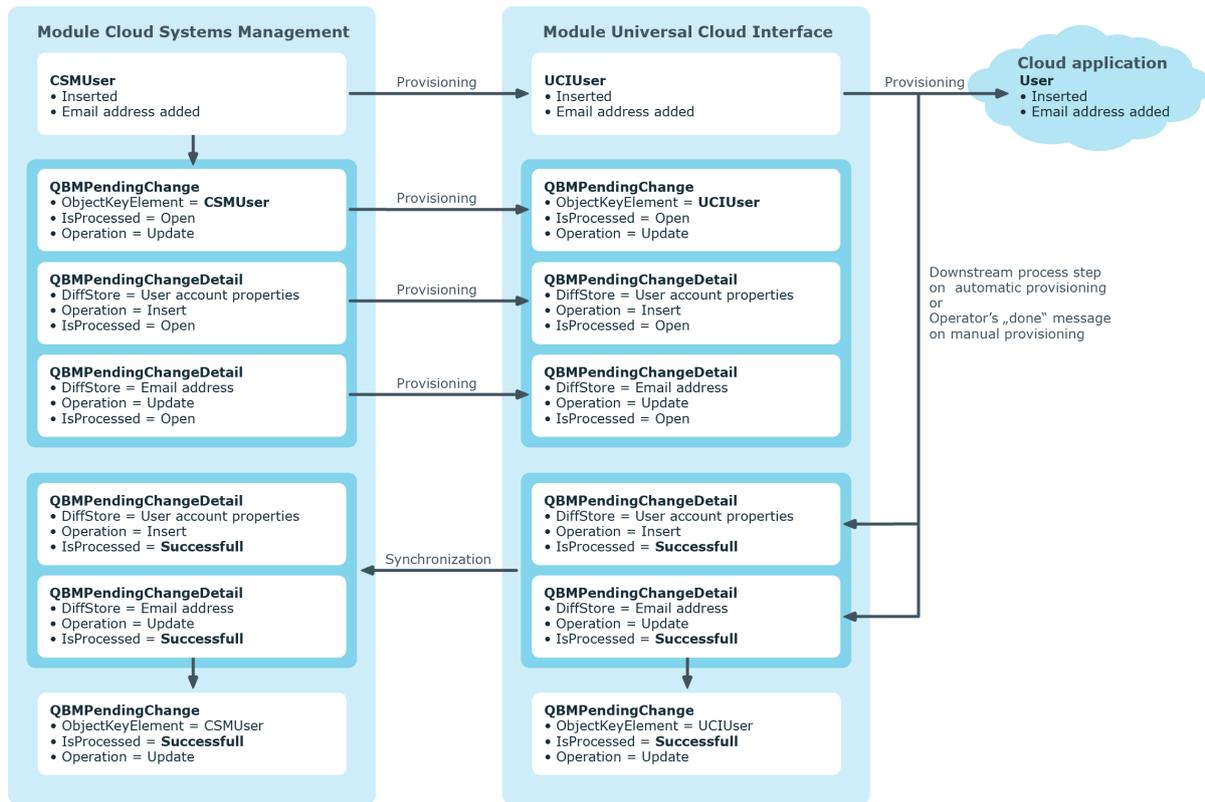
By default, the Cloud Systems Management module is synchronized hourly with the Universal Cloud Interface. This ensures that the processing state for pending changes is declared promptly in the Cloud Systems Management Module.

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** menu item.

Table 45: Meaning of the icons in the toolbar

Icon	Meaning
	Show selected object.
	Reload the data.

Retention time for pending changes

Table 46: 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 60 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 this period has expired, the entries are deleted by the DBQueue Processor from the `QBMPendingChange` and `QBMPendingChangeDetail` tables. 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, in the Designer, edit the value of the "QBM | PendingChange | LifeTimeSuccess" configuration parameter.

2. To change the retention period for failed provisioning processes, in the Designer, edit the value of the "QBM | PendingChange | LifeTimeError" configuration parameter.

3. To change the retention period for open provisioning processes, in the Designer, edit the value of the "QBM | PendingChange | LifeTimeRunning" configuration parameter.

4. Enter a retention period in days.

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 47: 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 that 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 contains 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 that are the result of manual operations in the target system rather than provisioned by One Identity Manager.
Show user accounts with	This report contains all user accounts in the target system

Report	Description
an above average number of system entitlements	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 **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 **My One Identity Manager**.

Related topics

Overview of all assignments

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

Examples

- If the report is created for a resource, all roles are determined in which there are employees with this resource.

- If the report is created for a group or another system entitlement, all roles are determined in which there are employees with this group or system entitlement.

- If the report is created for a compliance rule, all roles are determined in which there are employees who violate this compliance rule.

- If the report is created for a department, all roles are determined in which employees of the selected department are also members.

- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

To display detailed information about assignments

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

- Click the ⛁ **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain employees with the selected base object.

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

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

Figure 4: Toolbar of the Overview of all assignments report.

ⓘ 🖫 | 🗁 Used by ▾ | 🔻 | ▶ Department ▶ Dresden

Table 48: 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.

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 49: 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 this parameter require the database to be recompiled.
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 provide users with the login data for their user accounts. The **Employee - new user account created** mail template is used.
TargetSystem\CSM\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	This configuration parameter contains the name of the mail template sent to provide users with information about their initial password. The **Employee - initial password for new user account** mail template is used.
TargetSystem\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. The **Employee - new user account with default properties created** mail template is used.
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 are listed in a pipe (|) delimited list that is handled as a regular search pattern.

Default project template for cloud applications in the Universal Cloud Interface

A default project template ensures that all required information is added in 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 50: 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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

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

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

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

Index

synchronization workflow

    create 16, 25

T

target system manager 66

target system managers 8

target system synchronization 28

template

    IT operating data, modify 43

U

user account 81

    account manager 91

    administrative user account 82

    apply template 43

    assign employee 95

    assign extended properties 94

    assign group 93

    assign permissions control 94

    category 114

    default user accounts 82

    delete 100

    disable employee 99

    identity 82, 87

    lock 99

    login 90

    login name 87

    password 64, 90

        notification 65

    privileged user account 82, 87

    set up 86

    type 82

    unlock 99