One Identity Manager 8.0.3

Administration Guide for Connecting to Cloud Applications

Legend

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

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

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

One Identity Manager Administration Guide for Connecting to Cloud Applications
Updated - March 2019
Version - 8.0.3

Contents

1

Synchronizing Cloud Applications through the Universal Cloud Interface

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.

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. Data is exchanged between the Universal Cloud Interface and Cloud System Management modules by synchronization. Provisioning processes ensure that object changes are transferred from the Cloud Systems Management Module to the Universal Cloud Interface Module.

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

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

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

Architecture Overview

One Identity Manager knows two methods for exchanging data with a cloud application.

- Automatic synchronization and provisioning

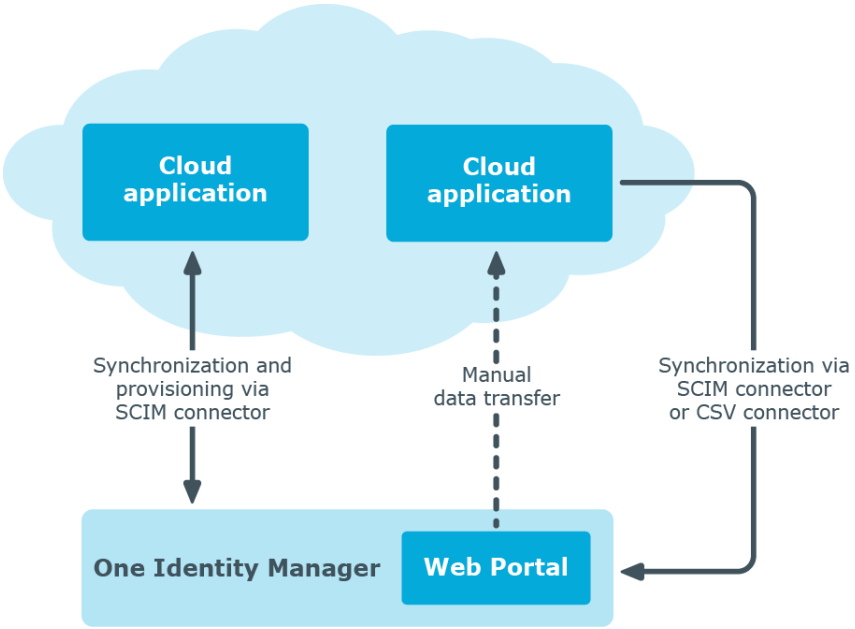
  The One Identity Manager SCIM connector is responsible for synchronizing a cloud application with the One Identity Manager database and for provisioning object changes from the One Identity Manager database to a cloud application. This default method ensures that target system and database data is regularly compared and therefore remains consistent.

- Manual provisioning

  Automated interfaces for provisioning changes from the to the cloud application can or should not be applied to certain cloud applications. Changes can be manually provisioned for cloud application like this. You can configure synchronization with the SCIM connector for exchanging data between the cloud application and the One Identity Manager database. If One Identity Manager cannot obtain read access to the cloud application, you can set up data exchange through the CSV connector, for example.

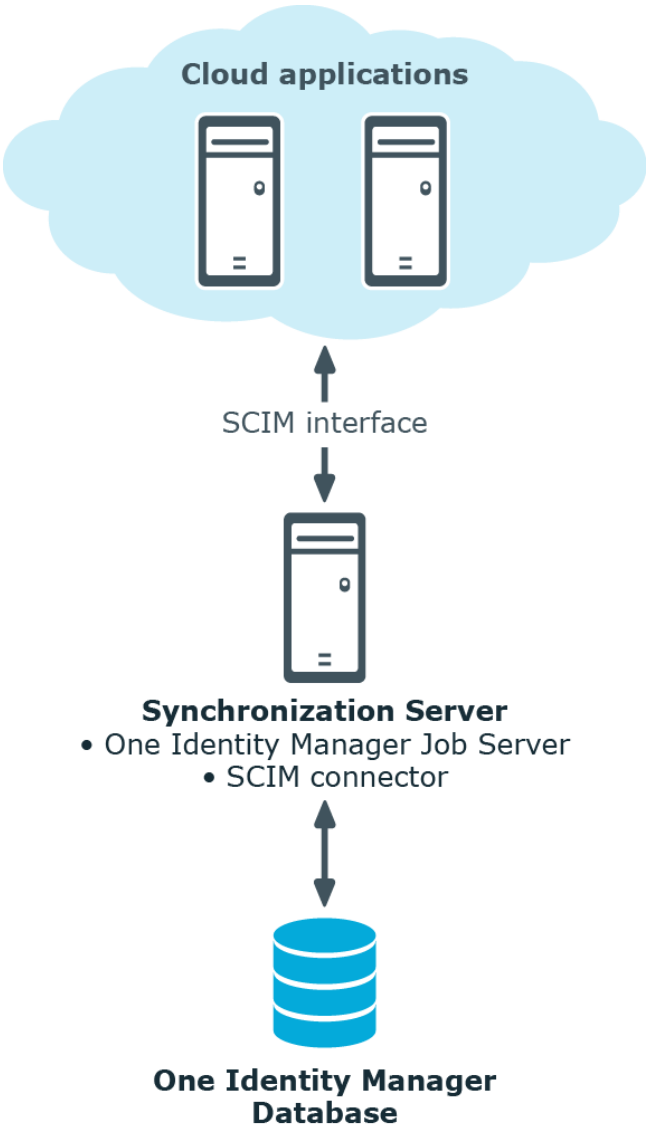
  With the method, you carry the risk of inconsistent data and loss of data if manual processes are not carried out. This method is, therefore, not recommended.

Figure 1: Architecture for synchronization



To access cloud applications, the SCIM connector is installed on a synchronization server. The SCIM connector can communicate with cloud applications, which understand the System for Cross-domain Identity Management (SCIM) specification. The synchronization server ensures data is compared between the One Identity Manager database and the cloud application.

Figure 2: Synchronization topology



Detailed information about this topic

- Setting up Synchronization with a Cloud Application on page 11
- Configuring Manual Provisioning on page 61

One Identity Manager Users for Managing Cloud Applications

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

Table 1: Users

User	Task
Administrators	Administrators must be assigned to the application **Universal Cloud Interface | Administrators** or a sub application role. Users with this application role: • Manage application roles for the Universal Cloud Interface. • Set up other application roles as required. • Configure synchronization in the Synchronization Editor and define the mapping for comparing tcloud applications and One Identity Manager. • Edit cloud application in the Manager. • Edit pending, manual provisioning processes in the Web Portal and obtain statistics. • Obtain information about the cloud objects in the Web Portal and the Manager.
Operators	Operators must be assigned to the application role **Universal Cloud Interface | Operators** or a sub application role. Users with this application role: • Edit pending, manual provisioning processes in the Web Portal and obtain statistics.
Auditors	Auditors must be assigned to the application role **Universal Cloud Interface | Auditors** or a sub application role. Users with this application role: • Can view manual provisioning processes in the Web Portal and obtain statistics.
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer, as required. • Create system users and permissions groups for non-role based login to administration tools, as required. • Enable or disable additional configuration parameters in

User	Task
	the Designer, as required. • Create custom processes in the Designer, as required. • Create and configures schedules, as required. • Create and configure password policies, as required.

2

Setting up Synchronization with a Cloud Application

One Identity Manager supports synchronization with cloud applications, which understand the System for Cross-domain Identity Management (SCIM) in the version 2.0 specification. One Identity Manager provides a project template that you can use to set up synchronization for the cloud applications.

To load cloud application objects into the One Identity Manager database for the first time.

1. Supply a user with sufficient permissions for accessing the cloud application.
2. Install and configure a synchronization server and declare the server as Job server in One Identity Manager.
3. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Users and Permissions for Synchronizing with a Cloud Application on page 11
- Setting Up a Synchronization Server on page 12
- Creating a Synchronization Project for Initial Synchronization of a Cloud Application on page 16

Users and Permissions for Synchronizing with a Cloud Application

The following users are involved in synchronizing One Identity Manager with a cloud application.

Table 2: Users for synchronization

User	Authorizations
One Identity Manager Service user account	The user account for the One Identity Manager Service requires access rights to carry out operations at file level (issuing user rights, adding directories and files to be edited). The user account must belong to the group "Domain Users". The user account must have the extended access right "Log on as a service". The user account requires access rights to the internal web service. NOTE: If the One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access rights for the internal web service with the following command line call: `netsh http add urlacl url=http://<IP address>:<port number>/ user="NT AUTHORITY\NETWORKSERVICE"` The user account needs full access to the One Identity Manager Service installation directory in order to automatically update the One Identity Manager. In the default installation the One Identity Manager is installed under: • `%ProgramFiles(x86)%\One Identity` (on 32-bit operating systems) • `%ProgramFiles%\One Identity` (on 64-bit operating systems)
Security tokens or users for accessing the cloud application	Security tokens or user name and password for use as authentication in the cloud application.
User for accessing the One Identity Manager database	The default system user "Synchronization" is available to run synchronization over an application server.

Setting Up a Synchronization Server

To set up synchronization with a cloud application, a server has to be available that has the following software installed on it:

- Windows operating system

  Following versions are supported:

    - Windows Server 2008 (non-Itanium based 64-bit) Service Pack 2 or later
    - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016
- Microsoft .NET Framework Version 4.5.2 or later

  NOTE: Microsoft .NET Framework version 4.6.0 is not supported.

  NOTE: Take the target system manufacturer's recommendations into account.
- Windows Installer
- One Identity Manager Service, Synchronization Editor, SCIM connector
    - Install One Identity Manager components with the installation wizard.
        1. Select the option **Select installation modules with existing database**.
        2. Select the machine role **Server | Job server | SCIM**.

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

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

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

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

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

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

a. Select a job server in the **Server** menu.

   - OR -

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

b. Enter the following data for the Job server.

Table 3: Job Servers Properties

Property	Description
Server	Name of the Job servers.
Queue	Name of queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Full server name	Full name of the server in DNS syntax. Example: `<name of server>.<fully qualified domain name>`

NOTE: Use the **Advanced** option to edit other Job server properties. You can use the Designer to change properties at a later date.

4. Specify which job server roles to include in One Identity Manager on the **Machine role** page. Installation packages to be installed on the Job server are found depending on the selected machine role.
   - SCIM
5. Specify the server's functions in One Identity Manager on the **Server functions** page. One Identity Manager processes are handled depending on the server function.

   The server's functions depend on which machine roles you have selected. You can limit the server's functionality further here.
   - SCIM connector
6. Check the One Identity Manager Service configuration on the **Service settings** page.

   NOTE: The initial service configuration is already predefined. If further changes need to be made to the configuration, you can do this later with the Designer. For more detailed information about configuring the service, see One Identity Manager Configuration Guide.
7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. Select the directory with the install files on the **Select installation source** page.

10. Select the file with the private key on the page **Select private key file**.

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

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

    Table 4: Installation Data

Data	Description
Computer	Server on which to install and start the service from. ***To select a server*** • Enter the server name. - OR - • Select a entry from the list.
Service account	One Identity Manager Service user account data. ***To enter a user account for the One Identity Manager Service*** • Set the option **Local system account**. This starts the One Identity Manager Service under the account "NT AUTHORITY\SYSTEM". - OR - • Enter user account, password and password confirmation.
Installation account	Data for the administrative user account to install the service. ***To enter an administrative user account for installation*** • Enable **Advanced**. • Enable the option **Current user**. This uses the user account of the current user. - OR - • Enter user account, password and password confirmation.

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

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

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

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

Creating a Synchronization Project for Initial Synchronization of a Cloud Application

Use the Synchronization Editor to set up synchronization between the One Identity Manager database and cloud application. 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.

NOTE: Be aware of case sensitive parts of the URL during configuration.

Table 5: Information Required for Setting up a Synchronization Project

Data	Explanation
Servers DNS name / URL	DNS name of the server that provides the SCIM interface or URL for connecting to the server.
Port	Port for accessing the cloud application.
URI service	URL for reaching the SCIM service.
Authentication endpoint or URL	URL available for authenticating. If authentication of another server or another root URL is used for authentication, the full URL must be entered here.
Authentication type	Permitted type of authentication for logging into the cloud application.
User account and password	User name and password for logging into the cloud application with the authentication types "Basic authentication", "OAuth authentication" and "Negotiated authentication".
Client secret	Security token for logging into the cloud application with the authentication type "OAuth authentication".
Application/Client ID	The application/client ID used to register the cloud application with the security token service. It is required for registering with the authentication type "OAuth-Authentication".
SCIM endpoint	Endpoint URIs or URLs for accessing the cloud application's schema, resource and service provider data.
Synchronization server	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data

<table>
<tr><th>Data</th><th>Explanation</th></tr>
<tr><td></td><td>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 SCIM connector must be installed on the synchronization server.

The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server.

Table 6: Additional Properties for the Job Server
<table><tr><th>Property</th><th>Value</th></tr><tr><td>Server Function</td><td>SCIM connector</td></tr><tr><td>Machine role</td><td>Server/Job server/SCIM</td></tr></table>
For more information, see Setting Up a Synchronization Server on page 12.</td></tr>
<tr><td>One Identity Manager Database Connection Data</td><td>SQL Server:
Database server
Database
Database user and password
Specifies whether Windows authentication is used.

This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Oracle:
Species whether access is direct or through the Oracle client

Which connection data is required, depends on how this option is set.
Database server
Oracle instance port
Service name
Oracle database user and password
Data source (TNS alias name from <code>TNSNames.ora</code>)</td></tr>
<tr><td>Remote connection</td><td>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity</td></tr>
</table>

Data	Explanation
server	Manager communicates directly with 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 to the workstation is not possible, you can set up a remote connection. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • `RemoteConnectPlugin` is installed • SCIM connector is installed The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required. For more detailed information about setting up a remote connection, see the One Identity Manager Target System Synchronization Reference Guide.

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

- In default mode
- Started from the launchpad

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

To set up initial synchronization project for a cloud application

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

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

2. Select the entry **SCIM interface target system type**. Click **Run**.

   This starts the Synchronization Editor's project wizard.

3. Specify how the One Identity Manager can access the target system on the **System access** page.

   - If you have access from the workstation from which you started the Synchronization Editor, do not set anything.

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

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

4. Enter the connection parameters required by the SCIM connector to log in on the cloud application on the **Configuration data** page.

Table 7: Server parameters

Property	Description
Servers DNS name / URL	DNS of the server, which provided by the SCIM interface or the URL for connecting to the server.
Port	Port for accessing the cloud application.
Service URI	URI for reaching the SCIM service. Only the part of the URL used in common by all endpoints to be called, is required. The SCIM connector take the URL from the server URL, the port and URI together. For example, if the full URL is "https://identities.example.net:8080/scim/v2", then enter "scim/v2" as the URI.

Table 8: Authentication type

Property	Description
Basic authentication	Authentication using user name and password.
OAuth authentication	Authentication using OAuth protocol 2.0.
Negotiated authentication	Authentication using Windows authentication methods like NTLM or Kerberos.
Authentication endpoint/URL	URI, under which authentication is possible. Only the part of the URL added to the common part, is required to reach the authentication endpoints. If authentication of another server or another root URL is used for authentication, the full URL must be entered here. Example: If the full URI is "https://identities.example.net:8080/scim/v2/auth/token", enter "auth/token" in this case. If the base URL or the server is different to the resource URL, enter the full URL, for example "https://authserver.example.net/token".

- Enter the user name and password for the authentication type "Basic authentication" on the page **Basic Authentication**.
- Enter the client secret for the authentication type "OAuth authentication" on the **OAuth Authentication page**.

Table 9: OAuth Authentification Properties

Property	Description
Security token	Security token for logging in to the cloud application. If the client secret is not known, enter the user name and password.
User account and password	User name and password for logging into the cloud application if the security token is not known.
Application/Client ID	The application/client ID used to register the cloud application with the security token service.
Grant type	Security token for logging into the cloud application with the authentication type "OAuth authentication". Enable **Client credentials** or **Password credentials**.

- Enter the user name and password for the authentication type "Negotiated authentication (NTLM/Kerberos)" on the **Negotiated authentication** page.

5. You can test the connection on **Verify connection settings** page. Click **Test**.

   One Identity Manager tries to connect to the cloud application.

   TIP: One Identity Manager saves the test result. When you reopen the page and the connection data has not changed, the result of the test is displayed. You do not have to run the connection test again if it was successful.

6. Enter the URIs of the SCIM endpoints on the **Endpoint Configuration** page. The SCIM default is used there is no URI.

Table 10: Endpoint Configuration

Property	Description
Schema	Endpoin for accessing the cloud application's schema information.
Resources	Endpoint for accessing cloud application resource data, for example, groups or user accounts.
Supported service options	Endpoint for accessing cloud application service provider data.

- To test the endpoint connections, click **Test**.

  TIP: One Identity Manager saves the test result. When you reopen the page and the endpoint configuration has not changed, the result of the test is displayed.

7. On the **Target product selection** page, you can customize how the SCIM connector behaves with the singularities of special target products, for example HTTP request formats.

   Table 11: Target Products

Property	Description
SCIM Core V 2.0	Product for synchronizing a default SCIM environment.
One Identity Connect For Cloud	Product for synchronizing a One Identity Connect For Cloud system

8. Enter a unique display name for the cloud application on the **Display name** page.

   You can use display names to differentiate between the cloud application in One Identity Manager tools. Display names cannot be changed later.

9. On the last page of the system connection wizard you can save the connection data locally and finish the system connection configuration.
   - Set the option **Save connection data on local computer** 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.

10. Verify the One Identity Manager database connection data on the **One Identity Manager connection** page. The data is loaded from the connected database. Reenter the password.

    NOTE: Reenter all the connection data if you are not working with an encrypted One Identity Manager database and no synchronization project has been saved yet in the database. This page is not shown if a synchronization project already exists.

11. 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.

12. Select a project template on the **Select project template** page to use for setting up the synchronization configuration.

Table 12: Default Project Templates

Project template	Description
SCIM synchronization	Use this project template for initially setting up the synchronization project for synchronizing a System for Cross-domain Identity Management environment.
Synchronizing a One Identity Connect For Cloud environment	Use this project template for initially setting up the synchronization project for synchronizing a SCIM environment using the One Identity Connect For Cloud infrastructure.

NOTE: A default project template ensures that all required information is added in the One Identity Manager. This includes mappings, workflows and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

13. Specify how system access should work on the page **Restrict target system access**. You have the following options:

Table 13: Specifying Target System Access

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

Option	Meaning
	ization steps in synchronization direction "target system". • Synchronization steps are only created for such schema classes whose schema types have write access.

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

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

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

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

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

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

    This creates and allocates a default schedule for regular synchronization. Enable the schedule for regular synchronization.

    The synchronization project is created, saved and enabled immediately.

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

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

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

To configure the content of the synchronization log

1. To configure the synchronization log for target system connection, select the category **Configuration | Target system**.
2. To configure the synchronization log for the database connection, select the category **Configuration | One Identity Manager connection**.
3. Select **General** view and click **Configure...**.
4. Select the **Synchronization log** view and set **Create synchronization log**.

5. Enable the data to be logged.

   NOTE: Certain content create a lot of log data.

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

6. Click **OK**.

To synchronize on a regular basis

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

To start initial synchronization manually

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

Detailed information about this topic

- One Identity Manager Target System Synchronization Reference Guide

Related Topics

- Setting Up a Synchronization Server on page 12
- Users and Permissions for Synchronizing with a Cloud Application on page 11
- Show Synchronization Results on page 24
- Customizing Synchronization Configuration on page 25
- Speeding Up Synchronization with Revision Filtering on page 28
- Additional Information for Experts on page 67
- Appendix: Default Project Template for Cloud Applications on page 69

Show Synchronization Results

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

To display a synchronization log

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

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

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

To display a provisioning log.

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

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

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

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

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

- In the Designer, set the "DPR\Journal\LifeTime" configuration parameter and enter the maximum retention time.

Customizing Synchronization Configuration

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

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

- Create a workflow with the direction of synchronization "target system" to use One Identity Manager as the master system for synchronization.
- To specify which cloud 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 which contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes or processing methods, for example.
- Update the schema in the synchronization project, if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

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

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

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

Detailed information about this topic

- How to Configure Cloud Application Synchronization on page 26
- Updating Schemas on page 27

How to Configure Cloud Application Synchronization

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

To create a synchronization configuration for synchronizing a cloud application

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

   This adds a workflow for synchronizing in the direction of the target system.

4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

Updating Schemas

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

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

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

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

To update a system connection schema

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

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

Speeding Up Synchronization with Revision Filtering

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

SCIM supports revision filtering. The cloud objects' date of last change is used as revision counter. Each synchronization save its last execution date as revision in 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 cloud 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 cloud application.

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

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

To permit revision filtering on a workflow

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

To permit revision filtering for a start up configuration

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

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

Configuring Memberships Provisioning

Memberships, for example, user accounts in groups, are saved in assignment tables in the One Identity Manager database. During provisioning of modified memberships, changes made in the target system will probably be overwritten. This behavior can occur under the following conditions:

- Memberships are saved in the target system as an object property in list form (Example: List of users accounts in the property `members~value` of a Cloud `group`).
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If a membership in One Identity Manager changes, the complete list of members is transferred to the target system by default. Memberships, previously added to the target system are removed by this; previously deleted memberships are added again.

To prevent this, provisioning can be configured such that only the modified membership is provisioned in the target system. The corresponding behavior is configured separately for each assignment table.

To allow separate provisioning of memberships

1. Start the Manager.
2. Select the category **Universal Cloud Interface | Basic configuration data | Target system types**.
3. Select **Configure tables for publishing**.
4. Select the assignment tables for which you want to allow separate provisioning. Multi-select is possible.
    - The option can only be set for assignment tables whose base table has a `XDateSubItem` or a `CCC_XDateSubItem`.
    - Assignment tables, which are grouped together in a virtual schema property in the mapping, must be labeled identically.
5. Click **Enable merging**.
6. Save the changes.

For each assignment table labeled like this, the changes made in the One Identity Manager are saved in a separate table. During modification provisioning, the members list in the target system is compared to the entries in this table. This means that only modified memberships are provisioned and the members list does not get entirely overwritten.

NOTE: The complete members list is updated by synchronization. During this process, objects with changes but incomplete provisioning are not handled. These objects are logged in the synchronization log.

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

Help for Analyzing Synchronization Issues

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

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

To generate a synchronization analysis report

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

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

Deactivating Synchronization

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

To prevent regular synchronization

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 loaded synchronization project

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

Detailed information about this topic

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

3

Base Data for Managing Cloud Applications

The following data is relevant for managing a cloud application in the One Identity Manager.

- Administrators

  In One Identity Manager, you can assign employees to any cloud application, who can configure synchronization of the cloud application with One Identity Manager. There is a default application role for administrators in One Identity Manager. Assign the employees to this application role, who are authorized to configure synchronization and run manual provisioning. Create more application roles if required.

  For more information, see Administrators on page 33.

- Operators

  In One Identity Manager, you can assign employees to any cloud application, who can execute manual provisioning. There is a default application role for operators in One Identity Manager. Create more application roles if required.

  For more information, see Operators on page 34.

- Auditors

  In One Identity Manager, you can assign employees to any cloud application, who can audit provisioning processes in the Web Portal. There is a default application role for auditors in One Identity Manager. Create more application roles if required.

  For more information, see Auditors on page 35.

- Servers

  Servers must know your server functionality in order to handle cloud specific processes in One Identity Manager. For example, the synchronization server.

  For more information, see Editing a Server on page 36.

Administrators

In One Identity Manager, you can assign employees to any cloud application, who can configure synchronization of the cloud application with One Identity Manager. There is a default application role for administrators in One Identity Manager. Assign the employees to this application role, who are authorized to configure synchronization and run manual provisioning. Create more application roles if required.

Table 14: Default Application Role for Administrators

User	Task
Administrators	Administrators must be assigned to the application **Universal Cloud Interface | Administrators** or a sub application role. Users with this application role: • Manage application roles for the Universal Cloud Interface. • Set up other application roles as required. • Configure synchronization in the Synchronization Editor and define the mapping for comparing tcloud applications and One Identity Manager. • Edit cloud application in the Manager. • Edit pending, manual provisioning processes in the Web Portal and obtain statistics. • Obtain information about the cloud objects in the Web Portal and the Manager.

To initially specify an employee as administrator

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

To edit administrators

1. Select the category **Universal Cloud Interface \| Basic configuration data \| Universal Cloud Interface managers \| Administrators**.
2. Select **Change master data** in the task view.

   - OR -

   Select an application role in the result list. Select **Change master data** in the task view.

- OR -

Click in the result list toolbar.

3. Edit the application role's master data.
   - Enter the application role name and assign the parent application role **Universal Cloud Interface | Administrators** or a child application role.
4. Save the changes.
5. Select the task **Assign employees**, to assign members to the application role.
6. Assign employees in **Add assignments**.

   - OR -

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

For more detailed information about setting up application roles, see the One Identity Manager Application Roles Administration Guide.

Related Topics

- Viewing and Editing Provisioning Processes on page 65

Operators

In One Identity Manager, you can assign employees to any cloud application, who can execute manual provisioning. There is a default application role for operators in One Identity Manager. Create more application roles if required.

Table 15: Default Application Role for Operators

User	Task
Operators	Operators must be assigned to the application role **Universal Cloud Interface | Operators** or a sub application role. Users with this application role: • Edit pending, manual provisioning processes in the Web Portal and obtain statistics.

TIP: If you want to limit access permissions for operators to individual cloud application, define child application roles for each cloud application.

To specify operators

1. Login to the Manager with the application role **Universal Cloud Interface | Administrators**.

2. Select the category **Universal Cloud Interface | Basic configuration data | Cloud application**.
3. Select the cloud application in the result list.
4. Select **Change master data** in the task view.
5. Select the application in **Operators** on the **General** tab.

   - OR -

   Click next to **Operators** to create a new application role.
   - Enter the application role name and assign the parent application role **Universal Cloud Interface | Operators**.
   - 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 cloud application in One Identity Manager.

NOTE: You can also specify operators for individual containers Operators of a container are authorized to edit manual provisioning processes. Specify operators for containers in the category **Universal Cloud Interface | <cloud application> | Container structure**

To add employees to an application role

1. Login to the Manager with the application role **Universal Cloud Interface | Administrators**.
2. Select **Assign employees** in the task view.
3. Assign the employees you want and save the changes.

Related Topics

- Cloud Application Master Data on page 41
- Container Structures in a Cloud Application on page 44
- Editing Pending Provisioning Processes on page 64

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

Auditors

In One Identity Manager, you can assign employees to any cloud application, who can audit provisioning processes in the Web Portal. There is a default application role for auditors in One Identity Manager. Create more application roles if required.

Table 16: Default Application Role for Auditors

User	Task
Auditors	Auditors must be assigned to the application role **Universal Cloud Interface | Auditors** or a sub application role. Users with this application role: • Can view manual provisioning processes in the Web Portal and obtain statistics.

To specify auditors

1. Login to the Manager with the application role **Universal Cloud Interface | Administrators**.
2. Select the category **Universal Cloud Interface | Basic configuration data | Universal Cloud Interface managers | Auditors**.
3. Select **Change master data** in the task view.

   - OR -

   Select an application role in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
4. Edit the application role's master data.
   - Enter the application role name and assign the parent application role **Universal Cloud Interface | Auditors** or a child application role.
5. Save the changes.
6. Select the task **Assign employees**, to assign members to the application role.
7. Assign employees in **Add assignments**.

   - OR -

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

Related Topics

- Viewing all Provisioning Processes on page 65

Editing a Server

In order to handle cloud 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:

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

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

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

To edit a Job server and its functions

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

Detailed information about this topic

- Master Data for a Job Server on page 37
- Specifying Server Functions on page 40

Related Topics

- Setting Up a Synchronization Server on page 12

Master Data for a Job Server

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

Table 17: Job Server Properties

Property	Meaning
Server	Job server name.
Full	Full server name in accordance with DNS syntax.

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

Property	Meaning
	This input is evaluated when One Identity Manager Service is automatically updated. If the server is handling several queues the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. Permitted values are "Win32", "Windows", "Linux" and "Unix". If the input is empty, "Win32" is assumed.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server) the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the procedure `QBM_PJobQueueLoad` the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in program "Job Queue Info".
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently being executed.
Server Function	Server functionality in One Identity Manager. One Identity Manager processes are handled depending on the server function.

Related Topics

- Specifying Server Functions on page 40

Specifying Server Functions

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

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

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

Table 18: Permitted Server Functions

Server Function	Remark
Update Server	This server executes automatic software updating of all other servers. The server requires a direct connection to the database server that the One Identity Manager database is installed on. The server can execute SQL tasks. The server with the installed One Identity Manager database, is labeled with this functionality during initial installation of the schema.
SQL processing server	This server can process SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
One Identity Manager Service installed	Server on which a One Identity Manager Service is installed.
SMTP host	Server from which the One Identity Manager Service sends email notifications. Prerequisite for sending mails using the One Identity Manager Service is SMTP host configuration.
Default report server	Server on which reports are generated.
SCIM connector	The server can connect to a cloud application.

Related Topics

- Master Data for a Job Server on page 37

Cloud Applications

NOTE: Use One Identity Manager to set up the cloud applications in the Synchronization Editor database.

The cloud application master data is displayed in the Manager. New cloud applications are set up by default with the Synchronization Editor. You can also add a cloud application in the Manager if required. Properties of existing cloud applications are maintained in cloud target systems in the Cloud Systems Management Module and transferred to the Universal Cloud Interface Module by provisioning. Operators must also assigned in the Manager for existing cloud application.

To edit cloud application master data

1. Select the category **Universal Cloud Interface | Basic configuration data | Cloud application**.
2. Select a cloud application in the result list. Select **Change master data** in the task view.
3. Edit the cloud application's master data.
4. Save the changes.

TIP: You can also display cloud application properties in the category **Universal Cloud Interface | <cloud application>**.

Detailed information about this topic

- Cloud Application Master Data on page 41
- Alternative Column Names on page 43

Cloud Application Master Data

Enter the following master data for a cloud application.

Table 19: Cloud Application Master Data

Property	Description
Cloud application	Name of the cloud application.
Canonical name	Full name of the cloud application. The canonical name is made up of the server's DNS name or it's URL respectively, the port and the service's URI. Example : `identities.example.net:8080/scim/v2`
Distinguished name	The cloud application's distinguished name. This distinguished name is used to form distinguished names for child objects. Syntax example: `DC = <canonical name>`
Display name	Name for displaying the cloud application in One Identity Manager tools.
Operators	Application role in which the operators are defined. Operator edit manual provisioning processes for the cloud application that they are assigned to. Every cloud application can be assigned to other operators. Select the One Identity Manager application, whose members are allowed to edit manual provisioning processes. Use the button to add a new application role.
Description	Spare text box 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. IMPORTANT: If you set this option, you ensure that by using regular and frequent synchronization, data remains consistent between the One Identity Manager database and the cloud application.
User account deletion not permitted	Specifies whether user accounts in the cloud application can be deleted. If this option is set, user account can only be disabled.

Related Topics

- Configuring Manual Provisioning on page 61
- Managing Provisioning Processes in the Web Portal on page 63

Alternative Column Names

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

To specify alternative column names

1. Select the category **Universal Cloud Interface | Basic configuration data | Cloud application**.
2. Select a cloud application in the result list. Select **Change master data** in the task view.
3. Select the tab **Alternative column names**.
4. Open the membership tree in the table whose column name you want to change.

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

How to Edit a Synchronization Project

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

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

To open an existing synchronization project in the Synchronization Editor

1. Select the category **Universal Cloud Interface | Basic configuration data | Cloud application**.
2. Select the cloud application in the result list. Select **Change master data** in the task view.
3. Select **Edit synchronization project...** from the task view.

Related Topics

- Customizing Synchronization Configuration on page 25

5

Container Structures in a Cloud Application

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

To display a containers master data

1. Select the category **Universal Cloud Interface | <cloud application> | Container structure**.
2. Select the container in the result list.
3. Select **Change master data** in the task view.

You are provided with the following master data for a container.

Table 20: 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 application	The container's cloud application.
Description	Spare text box for additional explanation.
Account manager	Manager responsible for the container.
Operators	Application role in which the operators are defined. Operators edit manual provisioning processes for the container that they are assigned to. Every container can be assigned to other operators. Select the One Identity Manager application, whose members are allowed to edit manual provisioning processes. Use the button to add a new application role.

Related Topics

- Operators on page 34

User Accounts in a Cloud Application

User accounts represent a cloud application's authentication objects. A user account obtains the required permissions for accessing cloud resources for its memberships in groups and control elements.

To display a user account's master data

1. Select the category **Universal Cloud Interface | <cloud application> | User accounts**.
2. Select the user account in the result list.
3. Select **Change master data** in the task view.

Related Topics

- Additional Master Data for a User Account on page 46
- User Account Login Data on page 48
- Identification Tasks on page 48
- Contact Data on page 49
- User Defined Master Data on page 49

Additional Master Data for a User Account

You are provided with the following general master data for a user account.

Table 21: Additional Master Data for a User Account

Property	Description
Cloud application	The user account's cloud application.

Property	Description
Form of address	User's form of address.
First name	The user’s first name.
Last name	The user’s last name.
Full name	Full name of the user account.
Initials	The user’s initials.
Job description	The user's job description.
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	User account's container.
First primary group	User account's primary group.
Second primary group	Additional primary group for the user account. If there are groups with different group types in the cloud application, another primary groups can be assigned.
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.
Resource type	Type of the resource, for example, `user`.
Description	Spare text box for additional explanation.
Login name	Name the user uses for logging into the cloud application.
User	Specifies that the user account is locked.

Property	Description
account is disabled	

User Account Login Data

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

Table 22: User Account Login Data

Property	Description
Password/Password confirmation	Password for the user account.
Password last changed	Date on which the password was last changed.
Last login	Date and time of the last login to the cloud application.

Identification Tasks

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

Table 23: Identification Data for a User Account

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

Property	Description
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.

Contact Data

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

Table 24: 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 25: Customized Master Data for a User Account

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

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

Additional Tasks for Managing User Accounts

The task view contains different forms with which you can run the following tasks.

Overview of User Accounts

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

To obtain an overview of a user account

1. Select the category **Universal Cloud Interface | <cloud application> | User accounts**.
2. Select the user account in the result list.
3. Select **User account overview** in the task view.

Assigning Groups

Use this task to view all the groups that are assigned to the user account.

To display assigned groups

1. Select the category **Universal Cloud Interface | <cloud application> | User accounts**.
2. Select the user account in the result list.
3. Select **Assign groups** in the task view.

Related Topics

- Groups in a Cloud Application on page 52

Assigning Permissions Controls

Use this task to view all the permissions controls that are assigned to the user account.

To display assigned permissions controls

1. Select the category **Universal Cloud Interface | <cloud application> | User accounts**.
2. Select the user account in the result list.
3. Select **Assign permissions controls**.

Related Topics

- Permissions Controls in a Cloud Application on page 56

Groups in a Cloud Application

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 display a group's master data

1. Select the category **Universal Cloud Interface | <cloud application> | Groups**.
2. Select the group in the result list.
3. Select **Change master data** in the task view.

Detailed information about this topic

- Entering Master Data for a Group on page 52
- User Defined Master Data for an Group on page 53

Entering Master Data for a Group

You are provided with the following general master data for a group.

Table 26: Entering Master Data for a Group

Property	Description
Name	Group identifier
Container	The group's container.
Cloud application	The group's cloud application.
Distinguished name	Distinguished name of the group.

Property	Description
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.
Description	Spare text box for additional explanation.
Group type	Name of the group type.
Resource type	Type of resource, for example, `Group`.

User Defined Master Data for an Group

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

Table 27: User Defined Master Data for an Group

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

Additional Tasks for Managing Groups

The task view contains different forms with which you can run the following tasks.

Overview of Groups

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

To obtain an overview of a group

1. Select the category **Universal Cloud Interface | <cloud application> | Groups**.
2. Select the group in the result list.
3. Select **Group overview** in the task view.

Assigning User Accounts

Use this task to view all user accounts that are assigned to groups.

To view assigned user accounts

1. Select the category **Universal Cloud Interface | <cloud application> | Groups**.
2. Select the group in the result list.
3. Select **Assign user accounts** in the task view.

Related Topics

- User Accounts in a Cloud Application on page 46

Assigning Groups

Use this task to view all groups that are assigned to groups.

To display assigned groups

1. Select the category **Universal Cloud Interface | <cloud application> | Groups**.
2. Select the group in the result list.
3. Select **Assign groups** in the task view.

Assigning Permissions Controls

Use this task to view all the permissions controls that are assigned to the group.

To display assigned permissions controls

1. Select the category **Universal Cloud Interface | <cloud application> | Groups**.
2. Select the group in the result list.
3. Select **Assign permissions controls**.

Related Topics

- Permissions Controls in a Cloud Application on page 56

8

Permissions Controls in a Cloud Application

Permissions controls map other cloud application objects.

To view a permissions control

1. Select the category **Universal Cloud Interface | <cloud application> | Permissions controls**.
2. Select the permissions control in the result list.
3. Select **Change master data** in the task view.

Detailed information about this topic

- General Master Data for Permissions Controls on page 56
- Custom Master Data for Permissions Controls on page 57

General Master Data for Permissions Controls

Enter the following master data for a permissions control.

Table 28: General Master Data for Permissions Controls

Property	Description
Cloud application	Cloud application in which the permissions control applies.
Permissions control	Name of the permissions control.
Access type	Additional permissions control properties.
Description	Spare text box for additional explanation.

Custom Master Data for Permissions Controls

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

Table 29: Custom Master Data for Permissions Controls

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

Additional Tasks for Permissions Controls

The task view contains different forms with which you can run the following tasks.

Permissions Control Overview

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

To obtain an overview of a permissions control

1. Select the category **Universal Cloud Interface | <cloud application> | Permissions controls**.
2. Select the permissions control in the result list.
3. Select **Permissions control overview** in the task view.

Assigning User Accounts

Use this task to view all user accounts that are assigned to the permissions control.

To view assigned user accounts

1. Select the category **Universal Cloud Interface | <cloud application> | Permissions controls**.
2. Select the permissions control in the result list.
3. Select **Assign user accounts** in the task view.

Related Topics

- User Accounts in a Cloud Application on page 46

Assigning Groups

Use this task to view all groups that are assigned to the permissions control.

To display assigned groups

1. Select the category **Universal Cloud Interface | <cloud application> | Permissions controls**.
2. Select the permissions control in the result list.
3. Select **Assign groups** in the task view.

Related Topics

- Groups in a Cloud Application on page 52

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. Automated interfaces for provisioning changes from the to the cloud application can or should not be applied to certain cloud applications. Changes can be manually provisioned for cloud application like this. Manual provisioning instances are displayed by a Web Portal. Operators can transfer pending changes to the cloud application on the basis of this overview.

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`. Pending changes are processed in the order in which they were created if provisioning is automatic. In the case of manual provisioning, the pending changes are listed in the order they were created in the Web Portal.

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

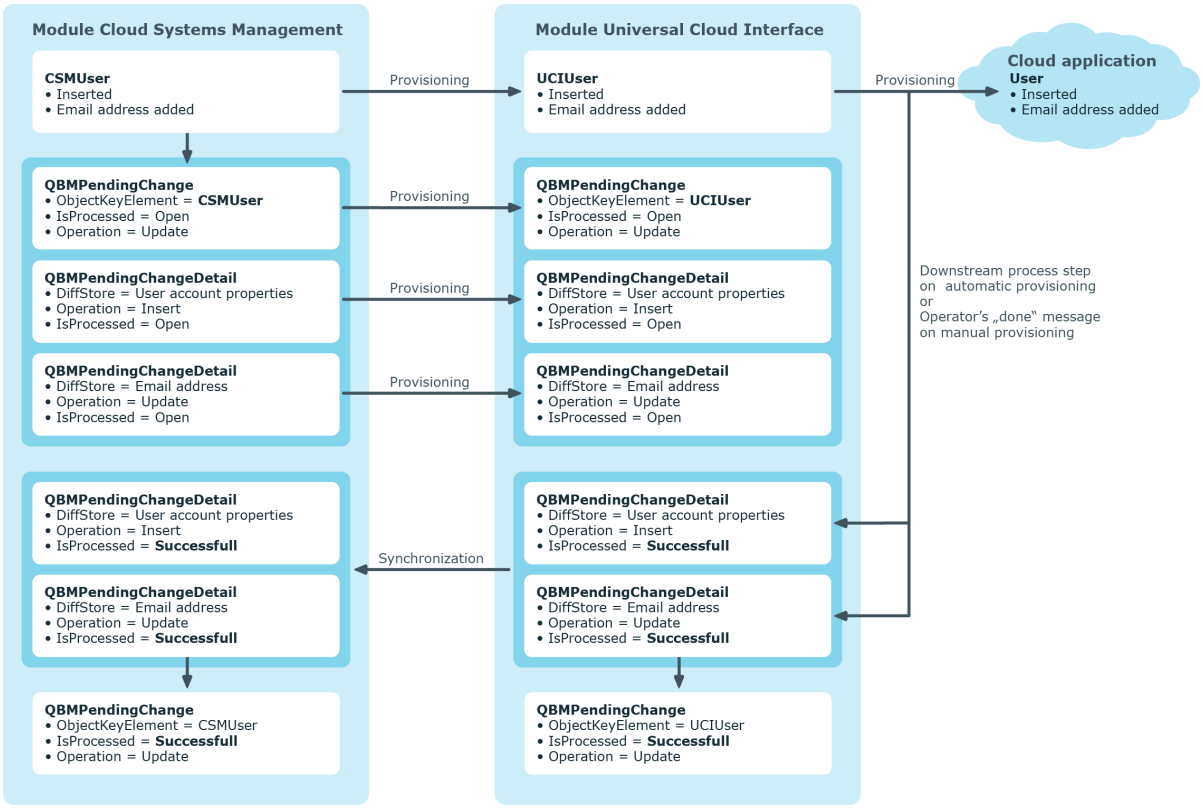
Detailed information about this topic

- The Provisioning Sequence on page 59
- Configuring Manual Provisioning on page 61
- Retention Time for Pending Changes on page 61

The Provisioning Sequence

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

Figure 3: Provisioning Sequence for Pending Changes



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

Displaying Pending Changes

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

To display pending changes

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

Table 30: Meaning of the Icons in the Toolbar

Icon	Meaning
	Show selected object.
	Reload the data.

Retention Time for Pending Changes

Table 31: Configuration Parameters

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

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

To configure the retention period for pending changes

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

Configuring Manual Provisioning

WARNING: **Data may be lost through inconsistencies.**

If you select manual provisioning, you must ensure that changes from the One Identity Manager database are transferred quickly to the cloud application using suitable manual processes.

Ensure that data between the cloud application and the One Identity Manager database is synchronized regularly and quickly. To do this, set up synchronization through the SCIM connector. If this is not possible, you can synchronize using the CSV connector.

Manual provisioning permissions are configured in the cloud application. Pending manual provisioning processes for this cloud application are displayed in the Web Portal. Operators can transfer pending changes to cloud application using this overview and then mark them as done. Auditors can check pending and completed provisioning processes in the Web Portal.

To configure manual provisioning

1. Edit the cloud application's master data.
    a. Set the option **Manual provisioning**.
    b. Assign operations, which are authorized to edit pending provisioning processes in the Web Portal.

        TIP: You can also specify operators for individual containers. For more information, see Container Structures in a Cloud Application on page 44.
2. Specify the auditors who are authorized to check manual provisioning processes in the Web Portal.

Detailed information about this topic

- Cloud Applications on page 41
- Cloud Application Master Data on page 41
- Operators on page 34
- Auditors on page 35
- Editing Pending Provisioning Processes on page 64
- Viewing all Provisioning Processes on page 65
- Setting up Synchronization with a Cloud Application on page 11

For more detailed information about synchronizing using the CSV connector, see the One Identity Manager CSV Connector User Guide.

10

Managing Provisioning Processes in the Web Portal

You can use the Web Portal to display pending manual provisioning processes for cloud applications. Operators can transfer pending changes to cloud application using this overview and then mark them as done. Auditors can check pending and completed provisioning processes in the Web Portal.

Users can view or manage their entitlements, provisioning processes in the Web Portal, depending on which application roles they own. For more information, see One Identity Manager Users for Managing Cloud Applications on page 9.

To log into the Web Portal

1. Type the Web Portal URL in the address bar to Open the Web Portal page.

   By default the URL is http: //<server name>/<application name>, where <server name> is the computer on which the Web Portal is installed.
2. Enter your complete login name in **Login name**.
3. Enter your password in **Password**.
4. Click **Log in**.

For more detailed information on login languages, see the One Identity Manager Web Portal User Guide in the Web Portal.

Detailed information about this topic

- Provisioning Object Changes on page 59
- Editing Pending Provisioning Processes on page 64
- Viewing and Editing Provisioning Processes on page 65
- Viewing all Provisioning Processes on page 65

Editing Pending Provisioning Processes

If you are an operator, you can edit pending provisioning processes in the Web Portal. A provisioning process is a work order for an operator to carry out an operation on a target system. There are the following target objects

Table 32: Target Objects

User account
Group
Assignment

NOTE: Administrators can also carry out pending provisioning processes.

The processes displayed in descending order by date with object names and a description of the operation in the **Pending cloud operations** view. The operation type is displayed in **Operation** in the detailed information about the marked process. There are the following operation types.

Table 33: Operation Types

New object	Create a new object.
Change	Set a value in the target system.
Deletion	Delete an object.

Detailed instructions are given in the operation detail for every requested operation labeled with . If several pending processes exist for one target object, you handle the processes in the order in which they arrived. That means the oldest process must be handled first.

To edit a pending provisioning process

1. Open the menu **Pending Cloud Operations** on the Web Portal's start page.
2. Mark the desired provisioning process in the **Pending Cloud Operations** view.

   NOTE: If several operations are list under each other for the pending process marked in the operation detail, edit the first operation.
3. Carry out the instructions.
4. Click **Mark as Done**.

   This causes the completed provisioning process to disappear from the **Pending Cloud Operations** view.

Viewing and Editing Provisioning Processes

You can view all provisioning processes as administrator. This means, you can see pending and closed processes. You can edit pending processes but you cannot edit failed provisioning processes. For more information, see Editing Pending Provisioning Processes on page 64.

To view provisioning processes

1. Open the menu **Cloud operations**

   This displays pending and closed provisioning processes in descending date order.
2. Perform one of the following tasks.
   a. Mark a pending processes and carry out the operation. Click **Mark as Done**.
   b. Mark the process and view the relevant information in the operation detail.

To view only provisioning processes.

1. Open the menu **Pending Cloud operations**
2. Edit the process and click **Mark as done**.

   Handled processes are moved to the **Cloud Operations** view.

Viewing all Provisioning Processes

You can view all provisioning processes in the Web Portal as an auditor. This means, you can see closed and pending provisioning processes. You cannot edit pending provisioning processes.

To view provisioning processes

1. Open the menu **Cloud operations**

   This displays pending and closed provisioning processes in descending date order.
2. Mark the process and view the relevant information in the operation detail.

Viewing Statistics

Statistics about provisioning processes are displayed on the Web Portal's start page and are visible for administrators, operators and auditors. The number of pending provisioning processes are displayed in chronological order in the statistics. The timeline consists of

point that represent each respective date and can be clicked on. Mouse over a point on the timeline to display a tooltip showing information about the pending processes on this tag.

To view statistics

1. Double-click on a point in the timeline.

   This opens a window with an enlarged visual. which makes the data for each point in the timeline viewable.

2. Mouse over the date above the point to you want to know about.

   The number of processes for this date are displayed.

3. Allow all processes with values to be displayed in decreasing chronological order.

   a. Click on the **Help** link.

   b. Select the **View source data** tab.

11

Additional Information for Experts

When you set up synchronization with a cloud application, One Identity Manager uses the SCIM schema exported from the server. If the SCIM connector cannot find the schema, you can pass it the schema data by using override files. The override files contain a complete description of the schema being used and they must confirm to the SCIM Core Schema specification (RFC 7643).

To configure synchronization with override files

1. Start the Synchronization Editor.
2. Enable expert mode.
3. Set up an initial synchronization project. For more information, see Creating a Synchronization Project for Initial Synchronization of a Cloud Application on page 16. The following anomalies apply:
    a. If you want more options, specify this on the **Export settings** page by setting **Show schema settings**.
    b. Enter the path for the override files on the **Schema definition** page. Both files must exist.

    Table 34: Override Files

Property	Description
Schema override file	Contains the complete schema definition of the cloud application.
Resource configuration override file	Contains a complete resource definition of the cloud application.

    - Click **Check** to check the override files for errors.

IMPORTANT: If override file are given in the synchronization configuration files they replace a schema definition on the server.

Schema definitions from override files are saved as connection parameters (`DPRSystemConnection.ConnectionParameter`).

You must make any changes to the SCIM schema in the override files, which must then be reloaded into the synchronization project.

To add schema changes to the synchronization project

1. Update the schema definition in the override files.
2. Open the synchronization project in the Synchronization Editor.
3. Enable expert mode.
4. Select the category **Configuration | Target systems**.
5. Select the **General** view and click **Edit connection...**.

   This starts the system connection wizard.
6. Enter the path for the override files on the **Schema definition** page.
7. End the system connection wizard.

   This updates the connection parameters.
8. Select the view **General** and click **Update schema**.
9. Confirm the security prompt with **Yes**.
10. Save the changes.

If the server has a valid schema definition because of later changes, for example, the override files' schema must be removed from the connection parameters.

To remove the override file's schema and apply the server's schema definition

1. Open the synchronization project in the Synchronization Editor.
2. Enable expert mode.
3. Select the category **Configuration | Target systems**.
4. Select the **General** view and click **Edit connection...**.

   This starts the system connection wizard.
5. Enter the URIs of the SCIM endpoints on the **Endpoint Configuration** page. Use the SCIM base schema if no URIs are given.
6. Select **Schema definition** and click **Clear existing** for both the schema override file and the resource configuration override file.
7. End the system connection wizard.
8. Select the view **General** and click **Update schema**.
9. Confirm the security prompt with **Yes**.
10. Save the changes.

Appendix: Default Project Template for Cloud Applications

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

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

The template uses mappings for the following schema types.

Table 35: Mapping SCIM schema types to tables in the One Identity Manager schema.

SCIM schema type	Table in the One Identity Manager schema
Group	UCIGroup
User	UCIUser

About us

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

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

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

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

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

Index

R

S

U