One Identity Manager 9.2

Administration Guide for Connecting to Cloud Applications

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

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

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

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

Patents

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

Trademarks

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

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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

One Identity Manager Administration Guide for Connecting to Cloud Applications
Updated - 29 September 2023, 05:18

For the most recent documents and product information, see Online product documentation.

Contents

Mapping cloud applications in One Identity Manager

One Identity Manager supports the implementation of Identity and Access Governance demands in IT environments, which are often a mix of traditional, on-premise 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 identity main 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 run 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, system entitlements, and permissions controls and can be organized into containers. They cannot be edited in One Identity Manager. There is no connection established to identities.

The connection to the identities is established in the Cloud Systems Management Module; user accounts, groups, system entitlements, 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.

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

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

Architecture overview

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

- Automatic synchronization and provisioning

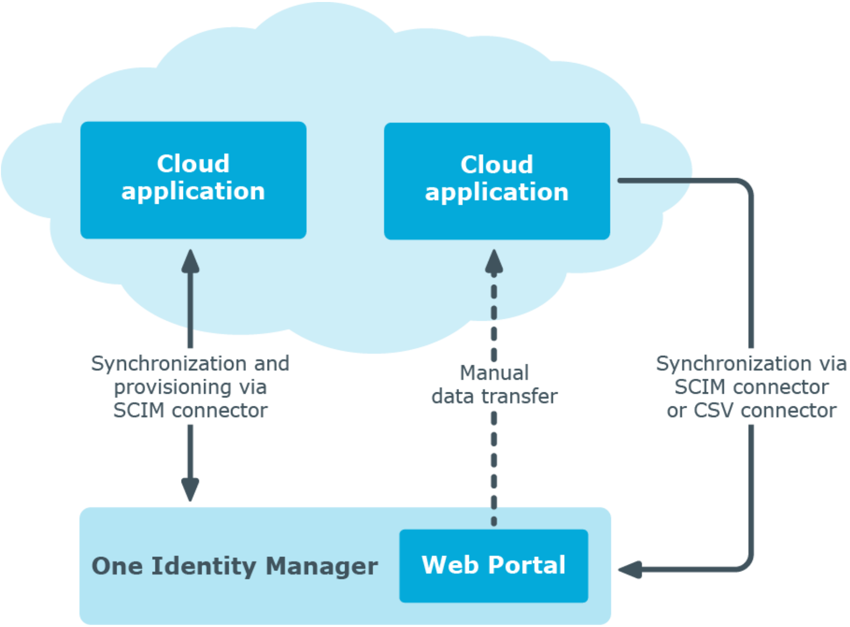
  Synchronizing a cloud application with the One Identity Manager database and provisioning changes to One Identity Manager database objects in the cloud application is handled by the One Identity Manager's SCIM connector. This standard procedure ensures that target system and database data is regularly compared and therefore remains consistent.

- Manual provisioning

  For certain cloud applications, automated interfaces for provisioning changes should not be implemented. Changes can be manually provisioned for cloud application like this. When data is transferred data from a cloud application to the One Identity Manager database, the synchronization can be configured with the SCIM connector. If One Identity Manager cannot obtain read access to the cloud application, you can set up data exchange through the CSV connector, for example.

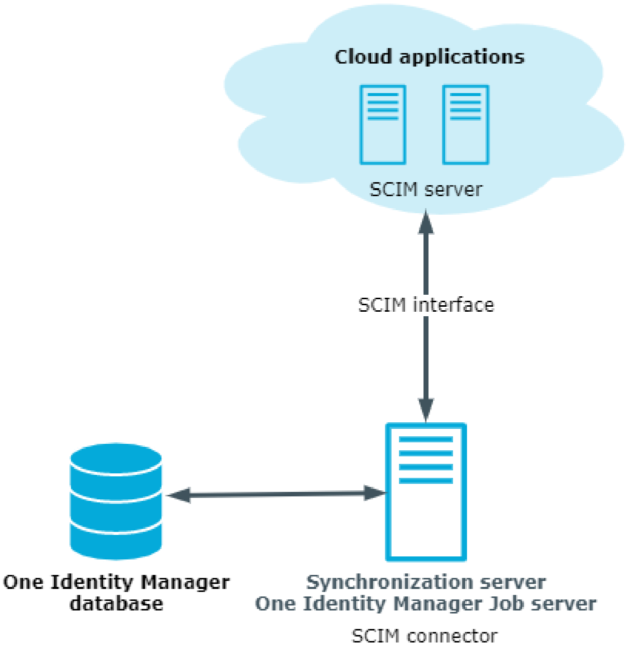
  With the method, you carry the risk of inconsistent data and loss of data if the manual processes are maintained. This method is therefore not recommended.

Figure 1: Architecture for synchronization


Cloud application
Cloud application
Synchronization and provisioning via SCIM connector
Manual data transfer
Synchronization via SCIM connector or CSV connector
One Identity Manager
Web Portal

To access cloud applications, the SCIM connector is installed on a synchronization server. The SCIM connector can communicate with cloud applications that 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 initial synchronization with a cloud application on page 13
- Configuring manual provisioning on page 52

One Identity Manager users for managing cloud applications

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

Table 1: Users

Users	Tasks
Cloud administrators	Cloud administrators must be assigned to the **Universal Cloud Interface | Administrators** application role

Users	Tasks
	or a child 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 cloud 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.
Cloud operators	The cloud operators must be assigned to the **Universal Cloud Interface | Operators** application role or a child application role. Users with this application role: • Edit pending, manual provisioning processes in the Web Portal and obtain statistics.
Cloud auditors	The cloud auditors must be assigned to the **Universal Cloud Interface | Auditors** application role or a child application role. Users with this application role: • Can view manual provisioning processes in the Web Portal and obtain statistics.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles. 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 in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required.

Users	Tasks
	• Create custom processes in the Designer as required. • Create and configure schedules as required.

2

Synchronizing cloud applications through the Universal Cloud Interface

One Identity Manager supports synchronization with cloud applications that understand the System for Cross-domain Identity Management (SCIM) in the version 2.0 specification. The requirements of RFC 7643 (System for Cross-domain Identity Management: Core Schema) and RFC 7644 (System for Cross-domain Identity Management: Protocol) must be guaranteed.

This sections explains how to:

- Set up synchronization to import initial data from cloud applications into the One Identity Manager database.
- Adapt a synchronization configuration to synchronize, for example, different cloud applications with the same synchronization project.
- Start and deactivate the synchronization.
- Evaluate the synchronization results.

> TIP: Before you set up synchronization with a cloud application, familiarize yourself with the Synchronization Editor. For more information about this tool, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Setting up initial synchronization with a cloud application on page 13
- Customizing the synchronization configuration on page 29
- Running synchronization on page 40
- Troubleshooting on page 44
- Cloud system object processing methods on page 94

Setting up initial synchronization with a cloud application

The One Identity Manager provides project templates with which you can set up synchronization of cloud applications. You use these project templates to create synchronization projects with which you import the data from a cloud application into your One Identity Manager database. In addition, the required processes are created that are used for the provisioning of changes to target system objects from the One Identity Manager database into the target system.

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 a 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 13
- Setting up the SCIM synchronization server on page 14
- Creating a synchronization project for initial synchronization of a cloud application on page 18
- Default project template for cloud applications on page 92

Users and permissions for synchronizing with a cloud application

The following users play a role in synchronizing One Identity Manager with a cloud application.

Table 2: Users for synchronization

User	Permissions
One Identity Manager Service user account	The user account for the One Identity Manager Service requires user permissions to carry out operations at file level (adding and editing directories and files). The user account must belong to the **Domain users** group.

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

Setting up the SCIM synchronization server

All One Identity Manager Service actions are run against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server.

The One Identity Manager Service must be installed on the synchronization server, with the SCIM connector.

Detailed information about this topic

- System requirements for the SCIM synchronization server on page 15
- Installing One Identity Manager Service with a SCIM connector on page 15

System requirements for the SCIM 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

  The following versions are supported:

  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Microsoft .NET Framework version 4.8 or later

  > NOTE: Take the target system manufacturer's recommendations into account.

Installing One Identity Manager Service with a SCIM connector

The One Identity Manager Service must be installed on the synchronization server with the SCIM connector. The synchronization server must be declared as a Job server in One Identity Manager.

Table 3: Properties of the Job server

Property	Value
Server function	SCIM connector
Machine role	Server | Job Server | SCIM

> NOTE: If several target system environments of the same type are synchronized under the same synchronization server, it is recommended that you set up a Job server for each target system for performance reasons. This avoids unnecessary swapping of connections to target systems because a Job server only has to process tasks of the same type (re-use of existing connections).

To set up a Job server, perform the following steps.

1. Create a Job server and install and configure the One Identity Manager Service.

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

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

Use the Server Installer to install the One Identity Manager Service locally or remotely.

To remotely install the One Identity Manager Service, provide an administrative workstation on which the One Identity Manager components are installed. Ensure that the One Identity Manager components are installed on the server before installing locally. For more information about installing One Identity Manager components, see the *One Identity Manager Installation Guide*.

2. If you are working with an encrypted One Identity Manager database, declare the database key in the One Identity Manager Service. For more information about working with an encrypted One Identity Manager database, see the *One Identity Manager Installation Guide*.
3. To generate processes for the Job server, you need the provider, connection parameters and the authentication data. By default, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For more information about connection data, see the *One Identity Manager Configuration Guide*.

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

1. Start the Server Installer program.

   > NOTE: To install remotely, start the Server Installer program on your administrative workstation. To install locally, start the program on the server.

2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.

   You can connect via the application server or directly to connect to the database.

3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.
   a. Select a Job server from the **Server** menu.

      - OR -

      To create a new Job server, click **Add**.
   b. Enter the following data for the Job server.
      - **Server**: Name of the Job server.
      - **Queue**: Name of the queue to handle the process steps. Each Job server within the network must have a unique queue identifier. The process

steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.

- **Full server name**: Full server name in accordance with DNS syntax.

  Syntax:

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

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

4. On the **Machine roles** page, select **SCIM**.
5. On the **Server functions** page, select **SCIM connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

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

   For a direct connection to the database:

   a. In the module list, select **Process collection > sqlprovider**.
   b. Click the **Connection parameter** entry, then click the **Edit** button.
   c. Enter the connection data for the One Identity Manager database.
   d. Click **OK**.

   For a connection to the application server:

   a. In the module list, select the **Process collection** entry and click the **Insert** button.
   b. Select **AppServerJobProvider** and click **OK**.
   c. In the module list, select **Process collection > AppServerJobProvider**.
   d. Click the **Connection parameter** entry, then click the **Edit** button.
   e. Enter the address (URL) for the application server and click **OK**.
   f. Click the **Authentication data** entry and click the **Edit** button.
   g. In the **Authentication method** dialog, select the authentication module for logging in. Depending on the authentication module, other data may be required, such as user and password. For more information about One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
   h. Click **OK**.
7. To configure the installation, click **Next**.

8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files. Change the directory if necessary.
10. On the **Service access** page, enter the service's installation data.
    - **Computer**: Select the server, on which you want to install and start the service, from the menu or enter the server's name or IP address.

      To run the installation locally, select **Local installation** from the menu.
    - **Service account**: Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

    The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options.

    You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced options.
11. Click **Next** to start installing the service.

    Installation of the service occurs automatically and may take some time.
12. Click **Finish** on the last page of the Server Installer.

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

Creating a synchronization project for initial synchronization of a cloud application

Use the Synchronization Editor to set up synchronization between the One Identity Manager database and cloud application. The following describes the steps for initial configuration of a synchronization project. For more information, see the *One Identity Manager Target System Synchronization Reference Guide*.

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.

Detailed information about this topic

- Information required for setting up a synchronization project on page 19
- Creating an initial synchronization project for a cloud application on page 21

Information required for setting up 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 4: Information required for setting up a synchronization project

Data	Explanation
URL of the SCIM server	URL used to connect to the server that deploys the SCIM interface. The URL must contain the transmission protocol in use.
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.
Public key for HPKP	Public key of the certificate to attach if you want to use the HPKP mechanism for limiting usage of the accepted certificate.
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 **Basic authentication**, **OAuth authentication**, and **Negotiated authentication** authentication types.
Client secret	Security token for logging into the cloud application with the **OAuth authentication** authentication type.
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 **OAuth authentication** authentication type.
Authentication token	Security token for logging into the cloud application with the **Bearer authentication** authentication type.
SCIM endpoint	Endpoint URIs or URLs for accessing the cloud application's schema, resource, and service provider data.
SCIM server's time zone	Time zone on which the SCIM provider bases its time data.
synchronization server	All One Identity Manager Service actions are run 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

Data	Explanation
	synchronization server. The One Identity Manager Service must be installed on the synchronization server with the SCIM connector. 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. • Server function: **SCIM connector** • Machine role: **Server/Jobserver/SCIM** For more information, see System requirements for the SCIM synchronization server on page 15.
One Identity Manager database connection data	• Database server • Database name • SQL Server login and password • Specifies whether integrated Windows authentication is used Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection. The remote connection server and the workstation must be in the same Active Directory domain. Remote connection server configuration: • One Identity Manager Service is started • **RemoteConnectPlugin** is installed • 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*.

Creating an initial synchronization project for a cloud application

> NOTE: The following sequence describes how to configure a synchronization project if the Synchronization Editor is both:
>
> - Run in default mode
> - Started from the Launchpad
>
> If you run the project wizard in expert mode or directly from the Synchronization Editor, additional configuration settings can be made. Follow the project wizard instructions through these steps.

> NOTE: Just one synchronization project can be created per target system and default project template used.

To set up initial synchronization project for a cloud application

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

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

2. Select the **Target system type SCIM interface** entry and click **Start**.

   This starts the Synchronization Editor's project wizard.

3. On the wizard's start page, click **Next**.
4. On the **System access** page, specify how One Identity Manager can access the target system.
   - If access is possible from the workstation on which you started the Synchronization Editor, do not change any settings.
   - If access is not possible from the workstation on which you started the Synchronization Editor, you can set up a remote connection.

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

5. On the **Certificate validation options** page, configure the certificate validation settings for encrypted connections.
   - If you want to use the HPKP mechanism for limiting usage of the accepted certificate, enter the certificate's public key.
6. On the **Connection data** page, enter the connection parameters required by the SCIM connector to login to the cloud application.

Table 5: Server parameters

Property	Description
Server's URL	URL for reaching the server. Enter the transfer protocol to use.
Port	Port for accessing the cloud application. This field can be left empty if default ports are used (HTTP:80, HTTPS:443).
URI of service	URL 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. Example: If the complete URL is https://identities.example.net:8080/scim/v2 then enter **scim/v2** as the URI.

Table 6: Authentication type

Property	Description
Basic authentication	Authentication with the user name and password.
OAuth authentifcation	Authentication with the OAuth protocol 2.0.
Negotiated authentication (NTLM/Kerberos)	Authentication using Windows authentication methods such as NTLM or Kerberos
Use client certificate	Authentication using a client certificate.
Bearer authentication	Authentication using an existing bearer token.
Authentication endpoint or URL	URL available for authenticating. 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** here. If the base URL or the server is different to the resource URL, enter the full URL, for example **https://authserver.example.net/token**. This URL is only used for testing the connection in all authentication modes apart from OAuth authentication.

- On the **Basic authentication** page, enter the user name and password for the **Basic Authentication** authentication type.
- On the **OAuth authentication** page, enter the security token for the **OAuth authentication** authentication type and select the access type.

Table 7: OAuth authentication properties

Property	Description
Client secret	Security token If the security token 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	Grant type for logging in to the cloud application with the **OAuth authentication** authentication type. Enable **Client credentials** or **Password credentials**.
Scope	Scope parameter valid for target system login. If several parameter apply, separate them with spaces. Whether a scope is required for logging in and which scope parameters are valid, depends on the service provider.

- On the **Negotiated authentication** page, enter the user name and password for the **Negotiated authentication (NTLM/Kerberos)** authentication type.
- On the **Client certificate** page, select the certificate you want to use. Certificates can imported into the local computer's certificate store from `*.CER` or `*.PFX` files.
- On the **Bearer authentication** page, enter the bearer token calculated by the target system.

7. On **Test connection settings** page, you can test the connection. 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.

8. On the **Endpoint configuration** page, enter the URIs for the SCIM end points. The SCIM default is used there is no URI.

Table 8: Endpoint configuration

Property	Description
Schema	Endpoint for accessing the cloud application's schema information.
Resources	End point for accessing the cloud application's resource information, such as groups or user accounts.
Supported service options	Endpoint for accessing the cloud application's service provider information.

a. To save endpoint data, click **Download**.

b. To test the connection at the specified end points, click **Test**.

> TIP: One Identity Manager saves the test result. If you reopen the page and the end point configuration has not changed, the save test result is displayed.

9. On the **Local cache** page, you can configure additional setting for optimizing synchronization performance.

Table 9: Performance optimization settings

Property	Description
Use local cache	Specifies whether the SCIM connector's local cache is used. Local cache is used to speed up synchronization. Access to the cloud application is minimized during full synchronization. The option is ignored during provisioning. This option is not set by default. NOTE: It does not make sense to use the cache when synchronization with revision filtering. If the target system supports revision filtering, disable the option after initial synchronization.
Max. number of parallel queries	Number of target system data queries that can be carried out at simultaneously. Enter a value between **1** and **32**.
Use HTTP Keep-Alive	Specifies whether HTTP connections are kept open. If the option is not set, connections are closed immediately and cannot be used for further queries.

10. On the **SCIM server time zone and time out settings** page, enter the time on which the SCIM provider bases its time data and configure the timeout for server queries.

- **SCIM server time zone**: If the SCIM provider supplies time and date values that do not contain any time zone information the time zone given here is used.
- **Timeout in ms (100,000 - 500,000)**: Maximum duration of a server request. If the time is exceeded, the request is canceled. The default value is **100,000 ms**. The maximum value is **500,000 ms**

11. 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 10: Target products

Property	Description
SCIM Core 2.0	Product for synchronizing a standard SCIM environment.
One Identity Starling Connect	Product for synchronizing a standard One Identity Starling Connect environment.

12. On the **Display name** page, enter a unique display name for the cloud application.

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

13. On the last page of the system connection wizard you can save the connection data locally and finish the system connection configuration.

    - Set the **Save connection data on local computer** option to save the connection data. This can be reused when you set up other synchronization projects.
    - Click **Finish**, to end the system connection wizard and return to the project wizard.

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

    NOTE:

    - If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all connection data again.
    - This page is not shown if a synchronization project already exists.

15. 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.

16. On the **Select project template** page, select a project template to use for setting up the synchronization configuration.

Table 11: Standard project templates

Project template	Description
SCIM synchronization	Use this project template for initial configuration of the synchronization project for synchronizing a System for Cross-domain Identity Management.
Synchronizing a One Identity Starling Connect environment	Use this project template for initial configuration of the synchronization project for synchronizing SCIM using One Identity Starling Connect infrastructure.

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

17. On the **Restrict target system access** page, specify how system access should work. You have the following options:

Table 12: Specify target system access

Option	Meaning
	Specifies that a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of **One Identity Manager**. • Processing methods in the synchronization steps are only defined for synchronization in the direction of **One Identity Manager**.
Read/write access to target system. Provisioning available.	Specifies whether a provisioning workflow is set up in addition to the synchronization workflow for the initial loading of the target system. The provisioning workflow displays the following characteristics: • Synchronization is in the direction of the **Target system**. • Processing methods are only defined in the

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

18. On the **Synchronization server** page, select the synchronization server to run the synchronization.

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

    a. Click + to add a new Job server.

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

       > TIP: You can also implement an existing Job server as the synchronization server for this target system.
       >
       > - To select a Job server, click 🪄.
       >
       > This automatically assigns the server function matching this Job server.

    c. Click **OK**.

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

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

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

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

    This sets up, saves and immediately activates the synchronization project.

    > NOTE:
    >
    > - If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide whether the synchronization project can remain activated or not.
    >
    >   Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor‛s start page, click **Verify project**.
    >
    > - If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically option**. In this case, save the synchronization project manually before closing the Synchronization Editor.

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

Detailed information about this topic

- System requirements for the SCIM synchronization server on page 15
- Users and permissions for synchronizing with a cloud application on page 13
- Displaying synchronization results on page 42
- Customizing the synchronization configuration on page 29
- Speeding up synchronization with revision filtering on page 34
- Synchronizing with override files on page 38
- Default project template for cloud applications on page 92

Configuring the synchronization log

All the information, tips, warnings, and errors that occur during synchronization are recorded in the synchronization log. You can configure the type of information to record separately for each system connection and synchronization workflow.

To configure the content of the synchronization log for a system connection

1. To configure the synchronization log for target system connection, in the Synchronization Editor, select the **Configuration > Target system** category.

   - OR -

   To configure the synchronization log for the database connection, in the Synchronization Editor, select the **Configuration > One Identity Manager connection** category.
2. In the **General** section, click **Setup**.
3. In the **Synchronization log** section, set **Create synchronization log**.
4. Enable the data to be logged.

   > NOTE: Some content generates a particularly large volume of log data. The synchronization log should only contain data required for error analysis and other analyzes.
5. Click **OK**.

To configure the content of the synchronization log for a synchronization workflow

1. In the Synchronization Editor, select the **Workflows** category.
2. Select a workflow in the navigation view.
3. In the **General** section, click **Edit**.

4. Select the **Synchronization log** tab.
5. Enable the data to be logged.

   > NOTE: Some content generates a particularly large volume of log data. The synchronization log should only contain data required for error analysis and other analyzes.

6. Click **OK**.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Related topics

- Displaying synchronization results on page 42

Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of a cloud application, You can use this synchronization project to load cloud application objects into the One Identity Manager cloud 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.

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- 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 that contain the necessary information about the synchronization objects when synchronization starts. Variables can be implemented in base objects, schema classes, or processing method, 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.

- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.
- Add your own schema types if you want to synchronize data that does not have schema types in the connector schema. Include the schema extensions in the mapping.
- If the SCIM connector cannot find the schema, pass it the schema data using overlay files.
- If the cloud application schema cannot be adequately represented by any default project template, customize the synchronization configuration. At the same time, define how the system entitlements are mapped in the One Identity Manager schema. When you are setting up synchronization, ensure that the base object for the cloud application(`CSMRoot`) is created in the database and the **System entitlements types used** (`GroupUsageMask`) and **User account has memberships** (`UserContainsGroupList`) properties are set correctly.

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

Detailed information about this topic

- Configuring cloud application synchronization on page 30
- Changing system connection settings of cloud applications on page 31
- Updating schemas on page 33
- Synchronizing with override files on page 38
- System entitlements types in cloud applications on page 67

Configuring cloud application synchronization

The synchronization project for initial synchronization provides a workflow for initial loading of target system objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). The synchronization project for initial synchronization provides a workflow for initial loading of Cloud objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). To use One Identity Manager as the primary system during synchronization, you also require a workflow with synchronization in the direction of the **Target system**.

To create a synchronization configuration for synchronizing a cloud application

1. In the Synchronization Editor, open the synchronization project.
2. Check whether the existing mappings can be used to synchronize into the cloud application. Create new maps if required.

3. Create a new workflow with the workflow wizard.

   This creates a workflow with **Target system** as its direction of synchronization.

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

Changing system connection settings of cloud applications

When you set up synchronization for the first time, the system connection properties are set to default values that you can modify. There are two ways to do this:

a. Specify a specialized variable set and change the values of the affected variables.

   The default values remain untouched in the default variable set. The variables can be reset to the default values at any time. (Recommended action).

b. Edit the target system connection with the system connection wizard and change the effected values.

   The system connection wizard supplies additional explanations of the settings. The default values can only be restored under particular conditions.

Detailed information about this topic

- Editing connection parameters in the variable set on page 31
- Editing target system connection properties on page 32

Editing connection parameters in the variable set

The connection parameters were saved as variables in the default variable set when synchronization was set up. You can change the values in these variables to suit you requirements and assign the variable set to a start up configuration and a base object. This means that you always have the option to use default values from the default variable set.

> NOTE: To guarantee data consistency in the connected target system, ensure that the start-up configuration for synchronization and the base object for provisioning use the same variable set.

To customize connection parameters in a specialized variable set

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.
3. Open the **Connection parameters** view.

Some connection parameters can be converted to variables here. For other parameters, variables are already created.

4. Select a parameter and click **Convert**.
5. Select the **Configuration > Variables** category.

   All specialized variable sets are shown in the lower part of the document view.
6. Select a specialized variable set or click on in the variable set view's toolbar.
   - To rename the variable set, select the variable set and click the variable set view in the toolbar . Enter a name for the variable set.
7. Select the previously added variable and enter a new value.
8. Select the **Configuration > Start up configurations** category.
9. Select a start up configuration and click **Edit**.
10. Select the **General** tab.
11. Select the specialized variable set in the **Variable set** menu.
12. Select the **Configuration > Base objects** category.
13. Select the base object and click .

    - OR -

    To add a new base object, click .
14. Select the specialized variable set in the **Variable set** menu.
15. Save the changes.

For more information about using variables and variable sets, or restoring default values and adding base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Editing target system connection properties on page 32

Editing target system connection properties

You can also use the system connection wizard to change the connection parameters. If variables are defined for the settings, the changes are transferred to the active variable set.

> NOTE: In the following circumstances, the default values cannot be restored:
>
> - The connection parameters are not defined as variables.
> - The default variable set is selected as an active variable set.
>
> In both these cases, the system connection wizard overwrites the default values. They cannot be restored at a later time.

To edit connection parameters using the system connection wizard

1. In the Synchronization Editor, open the synchronization project.
2. In the toolbar, select the active variable set to be used for the connection to the target system.

   > NOTE: If the default variable set is selected, the default values are overwritten and cannot be restored at a later time.
3. Select the **Configuration > Target system** category.
4. Click **Edit connection**.

   This starts the system connection wizard.
5. Follow the system connection wizard instructions and change the relevant properties.
6. Save the changes.

Related topics

- Editing connection parameters in the variable set on page 31

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

To update a system connection schema

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Target system** category.

   - OR -

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

   This reloads the schema data.

To edit a mapping

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

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

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

Speeding up synchronization with revision filtering

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

SCIM supports revision filtering. The cloud objects' date of last change is used as revision counter. Each synchronization saves the last date is was run as a revision in the One Identity Manager database (`DPRRevisionStore` table, `Value` column). 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 modified by synchronization are loaded and checked by the next synchronization. This means that the second synchronization after initial synchronization is not significantly faster.

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

To permit revision filtering on a workflow

- In the Synchronization Editor, open the synchronization project.
- Edit the workflow properties. Select the **Use revision filter** item from **Revision filtering** menu.

To permit revision filtering for a start up configuration

- In the Synchronization Editor, open the synchronization project.
- Edit the start up configuration properties. Select the **Use revision filter** item from the **Revision filtering** menu.

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

Configuring the provisioning of memberships

Memberships, such as 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 may be overwritten. This behavior can occur under the following conditions:

- Memberships are saved as an object property in list form in the target system.

  Examples: List of user accounts in the `members~value` property of a cloud group (`GROUP`) - OR - List of roles in a user's `roles~value` property `User`
- Memberships can be modified in either of the connected systems.
- A provisioning workflow and provisioning processes are set up.

If one membership in One Identity Manager changes, by default, the complete list of members is transferred to the target system. Therefore, memberships that were previously added to the target system are removed in the process and 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. In the Manager, select the **Universal Cloud Interface > Basic configuration data > Target system types** category.
2. In the result list, select the **SCIM interface** target system type.
3. Select the **Configure tables for publishing** task.
4. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.

5. Click **Merge mode**.

   > NOTE:
   >
   > - This option can only be enabled for assignment tables that have a base table with a `XDateSubItem` column.
   > - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.

6. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. Therefore, only newly added and deleted assignments are processed. 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 not the entire members list.

> 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.

You can restrict single provisioning of memberships with a condition. Once merge mode has been disabled for a table, the condition is deleted. Tables that have had the condition deleted or edited are marked with the following icon: ▦. You can restore the original condition at any time.

To restore the original condition

1. Select the auxiliary table for which you want to restore the condition.
2. Right-click on the selected row and select the **Restore original values** context menu item.
3. Save the changes.

> NOTE: To create the reference to the added or deleted assignments in the condition, use the `i` table alias.
>
> Example of a condition on the `UCIUserInGroup` assignment table:
>
> ```
> exists (select top 1 1 from UCIGroup g
>      where g.UID_UCIGroup = i.UID_UCIGroup
>      and <limiting condition>)
> ```

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

Configuring single object synchronization

Changes made to individual objects in the target system can be immediately applied in the One Identity Manager database without having to start a full synchronization of the target system environment. Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a membership list belongs to one of these properties, the entries in the assignment table will also be updated. If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

Prerequisites

- A synchronization step exists that can import the changes to the changed object into One Identity Manager.
- The path to the base object of the synchronization is defined for the table that contains the changed object.

Single object synchronization is fully configured for synchronization projects created using the default project template. If you want to incorporate custom tables into this type of synchronization project, you must configure single object synchronization for these tables. For more information about this, see the *One Identity Manager Target System Synchronization Reference Guide*.

To define the path to the base object for synchronization for a custom table

1. In the Manager, select the **Universal Cloud Interface > Basic configuration data > Target system types** category.
2. In the result list, select the **SCIM interface** target system type.
3. Select the **Assign synchronization tables** task.
4. In the **Add assignments** pane, assign the table for which you want to use single object synchronization.
5. Save the changes.
6. Select the **Configure tables for publishing** task.
7. Select the table and enter the **Root object path**.

   Enter the path to the base object in the ObjectWalker notation of the VI.DB.

   Example: `FK(UID_UCIRoot).XObjectKey`
8. Save the changes.

Related topics

- Synchronizing single objects on page 43

Accelerating provisioning and single object synchronization

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

> NOTE: You should not implement load balancing for provisioning or single object synchronization on a permanent basis. Parallel processing of objects might result in dependencies not being resolved because referenced objects from another Job server have not been completely processed.
>
> Once load balancing is no longer required, ensure that the synchronization server runs the provisioning processes and single object synchronization.

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
    - Job servers that share processing must have the **No process assignment** option enabled.
    - Assign the **SCIM connector** server function to the Job server.

    All Job servers must access the same cloud application as the synchronization server for the respective base object.
2. In the Synchronization Editor, assign a custom server function to the base object.

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

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

    For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.
3. In the Manager, assign this server function to all the Job servers that will be processing provisioning and single object synchronization for the base object.

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

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

To use the synchronization server without load balancing.

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

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

Detailed information about this topic

- Job server for cloud-specific process handling on page 82

Synchronizing with override files

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 18.

   The following special features apply:

   a. On the **Expert settings** page, define whether you want to make additional settings. Set the **Show schema settings** option.

   b. On the **Schema definition** page, enter the path for the override files. Both files must exist.

   - **Schema override file**: Contains the complete schema definition of the cloud application.
   - **Resource configuration override file**: Contains the full resource definition of the cloud application.

   c. To check the override files for errors, click **Check**.

> NOTE: 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. In the Synchronization Editor, open the synchronization project.
3. Enable expert mode.
4. Select the **Configuration > Target system** category.
5. Select the **General** view and click **Edit connection**.

   This starts the system connection wizard.
6. On the **Schema definition** page, enter the path for the override files.
7. End the system connection wizard.

   This updates the connection parameters.
8. Select the **General** view 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. In the Synchronization Editor, open the synchronization project.
2. Enable expert mode.
3. Select the **Configuration > Target system** category.
4. Select the **General** view and click **Edit connection**.

   This starts the system connection wizard.
5. Select the **Endpoint Configuration** page and enter the URIs for the SCIM end points. Use the SCIM base schema if no URIs are given.
6. Select the **Schema definition** page 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 **General** view and click **Update schema**.
9. Confirm the security prompt with **Yes**.
10. Save the changes.

Running synchronization

Synchronization is started using scheduled process plans. It is possible to start synchronization manually in the Synchronization Editor. You can simulate synchronization beforehand to estimate synchronization results and discover errors in the synchronization configuration. If synchronization stopped unexpectedly, you must reset the start information to be able to restart synchronization.

If you want to specify the order in which target systems are synchronized, use the start up sequence to run synchronization. In a start up sequence, you can combine start up configurations from different synchronization projects and specify the order in which they are run. For more information about start up sequences, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- Starting synchronization on page 41
- Deactivating synchronization on page 42
- Displaying synchronization results on page 42
- Synchronizing single objects on page 43
- Pausing handling of target system specific processes (Offline mode) on page 45

Starting synchronization

When you set up the initial synchronization project using the Launchpad, a default schedule for regular synchronization is created and assigned. Activate this schedule to synchronize on a regular basis.

To synchronize on a regular basis

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

You can also start synchronization manually if there is no active schedule.

To start initial synchronization manually

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
3. Select a start up configuration in the document view and click **Run**.
4. Confirm the security prompt with **Yes**.

> IMPORTANT: As long as a synchronization process is running, you must not start another synchronization process for the same target system. This especially applies, if the same synchronization objects would be processed.
>
> - If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.
>   - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
> - Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
>   - Use the schedule to ensure that the start up configurations are run in sequence.
>   - Group start up configurations with the same start up behavior.

Displaying synchronization results

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

To display a synchronization log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click ▶ in the navigation view toolbar.

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

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

To display a provisioning log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click ⚡ in the navigation view toolbar.

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

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

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

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

Related topics

- Configuring the synchronization log on page 28
- Troubleshooting on page 44

Deactivating synchronization

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

To prevent regular synchronization

1. In the Synchronization Editor, open the synchronization project.
2. Select the start up configuration and deactivate the configured schedule.

   Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

1. In the Synchronization Editor, open the synchronization project.
2. Select the **General** view on the home page.
3. Click **Deactivate project**.

Detailed information about this topic

- Creating a synchronization project for initial synchronization of a cloud application on page 18
- Pausing handling of target system specific processes (Offline mode) on page 45

Synchronizing single objects

Individual objects can only be synchronized if the object is already present in the One Identity Manager database. The changes are applied to the mapped object properties. If a membership list belongs to one of these properties, the entries in the assignment table will also be updated.

> NOTE: If the object is no longer present in the target system, then it is deleted from the One Identity Manager database.

To synchronize a single object

1. In the Manager, select the **Universal Cloud Interface** category.
2. Select the object type in the navigation view.
3. In the result list, select the object that you want to synchronize.
4. Select the **Synchronize this object** task.

   A process for reading this object is entered in the job queue.

Features of synchronizing memberships

If you synchronize changes in an object's member list, run single object synchronization on the assignment's root object, The base table of an assignment contains an `XDateSubItem` column containing information about the last change to the memberships.

> **Example:**
>
> Base object for assigning user accounts to groups is the group.
>
> In the target system, a user account was assigned to a group. To synchronize this assignment, in the Manager, select the group that the user account was assigned to and run single object synchronization. In the process, all of the group's memberships are synchronized.
>
> The user account must already exist as an object in the One Identity Manager database for the assignment to be made.

Detailed information about this topic

- Configuring single object synchronization on page 36

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- Simulating synchronization

  The simulation allows you to estimate the result of synchronization. This means you can, for example, recognize potential errors in the synchronization configuration.
- Analyzing synchronization

  You can generate the synchronization analysis report for analyzing problems which occur during synchronization, for example, insufficient performance.
- Logging messages

  One Identity Manager offers different options for logging errors. These include the synchronization log, the log file for One Identity Manager Service, the logging of messages with NLOG, and similar.
- Reset start information

  If synchronization stopped unexpectedly, for example, because a server was not available, the start information must be reset manually. Only then can the synchronization be restarted.

For more information about these topics, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Displaying synchronization results on page 42

Ignoring data error in synchronization

By default, objects with incorrect data are not synchronized. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be necessary to synchronize objects like these and ignore the data properties that have errors. This synchronization behavior can be configured in One Identity Manager.

To ignoring data errors during synchronization in One Identity Manager

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > One Identity Manager connection** category.
3. In the **General** view, click **Edit connection**.

   This starts the system connection wizard.
4. On the **Additional options** page, enable **Try to ignore data errors**.

   This option is only effective if **Continue on error** is set in the synchronization workflow.

   Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.
5. Save the changes.

> IMPORTANT: If this option is set, One Identity Manager tries to ignore commit errors that could be related to data errors in a single column. This causes the data changed in the affected column to be discarded and the object is subsequently saved again. This effects performance and leads to loss of data.
>
> Only set this option in the exceptional circumstance of not being able to correct the data before synchronization.

Pausing handling of target system specific processes (Offline mode)

If a target system connector is not able to reach the target system temporarily, you can enable offline mode for the target system. This stops target system specific processes from being frozen and having to be manually re-enabled later.

Whether offline mode is generally available for a target system connection is set in the base object of the respective synchronization project. Once a target system is truly unavailable, the target system connection can be switched offline and online again with the Launchpad.

In offline mode, all Job servers assigned to the base object are stopped. This includes the synchronization server and all Job servers involved in load balancing. If one of the Job servers also handles other tasks, these are not processed either.

Prerequisites

Offline mode can only be specified for a base object if certain prerequisites are fulfilled.

- The synchronization server is not used for any other base object as a synchronization server.
- If a server function is assigned to the base object, none of the Job servers with this server function may have any other server function (for example, update server).
- A dedicated synchronization server must be set up to exclusively process the Job queue for this base object. The same applies to all Job servers that are determined by the server function.

To allow offline mode for a base object

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Base objects** category.
3. Select a base object in the document view and click ✎.
4. Enable **Offline mode available**.
5. Click **OK**.
6. Save the changes.

> IMPORTANT: To prevent data inconsistencies, the offline phase should be kept as short as possible.
>
> The number of processes to handle depends on the extent of the changes in the One Identity Manager database and their effect on the target system during the offline phase. To establish data consistency between the One Identity Manager database and the target system, all pending processes must be handled before synchronization can start.
>
> Only use offline mode, if possible, for short system downtimes such as maintenance windows.

To flag a target system as offline

1. Start the Launchpad and log in on the One Identity Manager database.
2. Select **Manage > System monitoring > Flag target systems as offline**.
3. Click **Run**.

   This opens the **Manage offline systems** dialog. The **Base objects** section displays the base objects of target system connections that can be switched to offline.
4. Select the base object whose target system connection is not available.
5. Click **Switch offline**.
6. Confirm the security prompt with **OK**.

This stops all the Job servers assigned to the base object. No more synchronization or provisioning Jobs are performed. The Job Queue Info program shows when a Job server has been switched offline and the corresponding tasks are not being processed.

For more information about offline mode, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Deactivating synchronization on page 42

Assigning default profiles to user accounts in Salesforce applications

Cloud applications such as Salesforce require a system entitlement with a specific type to be already assigned when new user accounts are created. To this purpose, a default profile is automatically assigned to cloud user accounts when they are created in One Identity Manager.

Prerequisites

- Synchronization of a cloud application with the SCIM connector is set up in Universal Cloud Interface. When creating the synchronization project, the target product One Identity Starling Connect was selected and the **One Identity Starling Connect synchronization** project template was used.
- The target system was initially synchronized.
- Cloud application synchronization is set up in Cloud Systems Management Module.
- The cloud target system was initially synchronized.
- In the canonical name or display name of the cloud target system, the string **Salesforce** is used.
- There is a Cloud system entitlement 2 to be used as the default profile. The system entitlement name is entered for this system entitlement (`CSMGroup2.GroupName`).

To change the default profile for new user accounts

- In the Designer, edit the value of the **TargetSystem | CSM | ApplicationType | Salesforce | DefaultProfileName** configuration parameter and enter the name of the system entitlement 2, which is then assigned automatically to all new user accounts.

NOTE: By default, the mapping in Universal Cloud Interface is transferred to the cloud application by the `vrtProfileFirst profiles~value` property mapping rule in the **user** mapping. If the default profile in the cloud application is stored in a different schema property, adjust the property mapping rule accordingly.

TIP: If you do not want a default profile to be automatically assigned to new user accounts, disable the **TargetSystem | CSM | ApplicationType | Salesforce | DefaultProfileName** configuration parameter in the Designer.

3

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. For certain cloud applications, automated interfaces for provisioning changes should not be implemented. Changes can be manually provisioned for cloud application like this. The manual provisioning processes are displayed over the Web Portal. Operators can transfer pending changes to the cloud application on the basis of this overview.

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

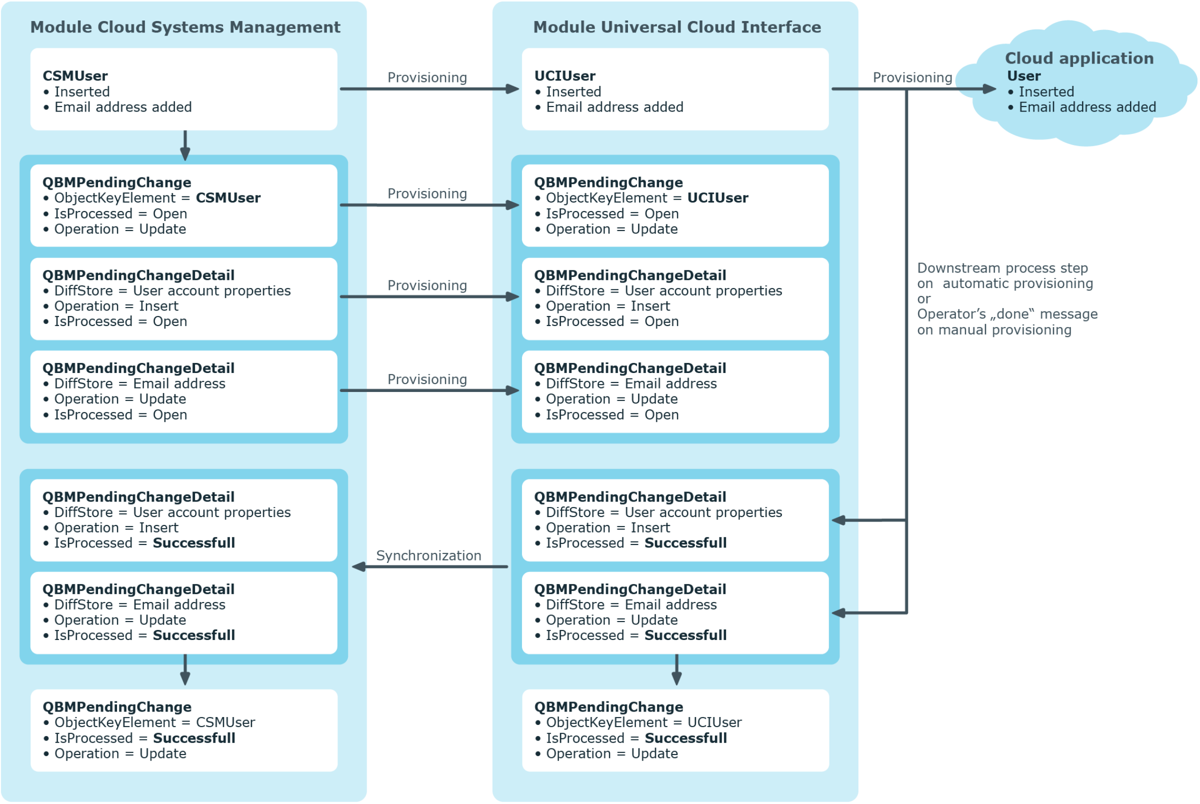
Detailed information about this topic

- The provisioning sequence on page 49
- Configuring manual provisioning on page 52
- Retention time for pending changes on page 51

The provisioning sequence

The following visual shows 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 not depend on whether the Cloud System Management and the Universal Cloud Interface modules 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.

Related topics

- Provisioning object changes on page 49

Displaying pending changes

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

To display pending changes

- In the Manager, select the **Database > Pending changes** menu item.

Table 13: Meaning of the icons in the toolbar

Icon	Meaning
🔍	Show selected object.
🔄	Reload the data.

Related topics

- Provisioning object changes on page 49

Retention time for pending changes

Pending changes are saved for a fixed period. After this period has expired, the entries are deleted by the DBQueue Processor from the `QBMPendingChange` and `QBMPendingChangeDetail` tables. The retention period depends on the status of provisioning processes and can be configured in the configuration parameter. The specified 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, in the Designer, edit the value of the **QBM | PendingChange | LifeTimeSuccess** configuration parameter. Enter a retention period in days. The default is **2** days.
2. To change the retention period for failed provisioning processes, in the Designer, edit the value of the **QBM | PendingChange | LifeTimeError** configuration parameter and enter the retention period in days. The default is **30** days.
3. To change the retention period for pending provisioning processes, in the Designer, edit the value of the **QBM | PendingChange | LifeTimeRunning** configuration parameter and enter the retention period in days. The default is **60** days.

Related topics

- Provisioning object changes on page 49

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 main data.
   a. Set the **Manual provisioning** option.
   b. In the Web Portal, assign the operators who are permitted to edit pending provisioning processes.

      > TIP: You can also specify operators for individual containers. For more information, see Container structures in cloud applications on page 61.
2. In the Web Portal, specify the auditors who are authorized to check manual provisioning processes.

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

Detailed information about this topic

- Editing cloud applications on page 58
- General main data for cloud applications on page 58
- Cloud operators on page 88
- Cloud auditors on page 89
- Editing pending provisioning processes on page 54
- Viewing all provisioning cases on page 55
- Setting up initial synchronization with a cloud application on page 13

Managing provisioning processes in the Web Portal

Pending manual provisioning processes for cloud applications 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.

Depending on which application roles they own, users can view or manage provisioning processes in the Web Portal according to their entitlements. For more information, see One Identity Manager users for managing cloud applications on page 9.

To log into the Web Portal

1. Open the Web Portal page by entering the Web Portal URL in the address bar of the web browser.

   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 the **Login name** field.
3. Enter your password in the **Password** field.
4. Click **Log in**.

For more information about logging in to the Web Portal, see in the *One Identity Manager Web Designer Web Portal User Guide*.

Detailed information about this topic

- Provisioning object changes on page 49
- Editing pending provisioning processes on page 54
- Viewing and editing provisioning processes on page 54
- Viewing all provisioning cases on page 55

Editing pending provisioning processes

If you are an operator, you can edit pending provisioning processes in the Web Portal. A provisioning process is a task for the operator to perform an operation on a target object.

> 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 the **Operation** view in the detailed information about the marked process. There are the following operation types.

Table 14: 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 ℹ. 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. On the Web Portal's home page, open the **Pending Cloud Operations** menu.
2. In the **Pending Cloud Operations** view, mark the desired provisioning process.

   > 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 54.

To view provisioning processes

1. Open the **Cloud Operations** menu.

   This displays pending and closed provisioning processes in descending date order.

2. Perform one of the following tasks:

   a. Mark the pending process and carry out the operation. Click **Mark as Done**.

   b. Mark the process and view the relevant information in the detailed information.

To view only provisioning processes.

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

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

Viewing all provisioning cases

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 **Cloud Operations** menu.

   This displays pending and closed provisioning processes in descending date order.

2. Mark the process and view the relevant information in the detailed information.

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 on the timeline in the graphical display.

   This opens a window with an enlarged graphic. making the data viewable at each point in the timeline.

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 **Show source** tab.

5

Mapping cloud objects in One Identity Manager

You can use One Identity Manager to manage users and entitlements in cloud applications. Each cloud application is mapped as its own base object in One Identity Manager. The user data is saved as user accounts, groups, system entitlements, and permissions controls and can be organized into containers.

Detailed information about this topic

- Editing cloud applications on page 58
- Container structures in cloud applications on page 61
- User accounts in cloud applications on page 62
- Groups in cloud applications on page 69
- Permissions controls in a cloud application on page 77
- Berichte über Objekte in Cloud Zielsystemen

Cloud applications

Each cloud application is mapped as its own base object in One Identity Manager. The cloud application main data is displayed in the Manager. Here you can assign the operators.

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.

> NOTE: The Synchronization Editor sets up the cloud applications in the One Identity Manager database.

Detailed information about this topic

- Editing cloud applications on page 58

Editing cloud applications

The cloud application general main data is displayed in the Manager. Here you can assign the operators and specify alternative column names. You can also add a cloud application in the Manager if required.

To display the main data of a cloud application and assign operators

1. In the Manager, select the **Universal Cloud Interface > Basic configuration data > Cloud applications** category.
2. Select a cloud application in the result list.
3. Select the **Change main data** task.
4. To handle provisioning processes manually in the Web Portal, select an application role for operators in the **Operator** field.
5. Save the changes.

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

Detailed information about this topic

- General main data for cloud applications on page 58
- Specifying alternative names on page 60

General main data for cloud applications

The following general main data is displayed for a cloud application. To handle manual provisioning operations, assign an application role for operators.

Table 15: Cloud application main 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>`

Property	Description
Display name	Name for displaying the cloud application in One Identity Manager tools.
Operator	Application role in which the cloud 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.
Types of system entitlements used	Types of system entitlements to which user accounts can be assigned in this cloud application.
User account has memberships	Specifies for which types of system entitlements, assignments are maintained in the user accounts. Example: In the **System entitlement types used** menu, the values **Group** and **System entitlement 1** are selected. In the **User account has memberships** menu, only the value **System entitlement 1** is selected. The assignments of user accounts to groups are saved with the groups, the assignment of user accounts to system entitlements 1 are saved with the user accounts.
Description	Text field for additional explanation.
Manual provisioning	Specifies whether changes to cloud objects in the One Identity Manager database are automatically provisioned in the cloud application. If this option is not set, processes for automatic provisioning of object modifications are configured. Set this option, if object modifications are not allowed to be published automatically in the cloud application. Use the Web Portal to transfer the changes to the cloud application. IMPORTANT: If you set this option, you must perform regular and frequent synchronization to ensure that 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 52
- Managing provisioning processes in the Web Portal on page 53
- System entitlements types in cloud applications on page 67

Specifying alternative names

You can use alternative names for each cloud application to improve how different objects types of a cloud application are presented.

Alternative names for tables are used for displaying object types in the Manager's navigation, as list titles for result lists or on the overview forms, for example, and alternative names for columns can be used for displaying input fields on main data forms or overview forms.

To specify alternative column names

1. In the Manager, select the **Universal Cloud Interface > Basic configuration data > Cloud applications** category.
2. In the result list, select a cloud application and select the **Change main data** task.
3. Switch to the **Alternative names** tab.

   This displays all the default names for the tables and columns.
4. Enter any name in the login language in use.
5. Save the changes.

Editing the synchronization project for a cloud application

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

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

To open an existing synchronization project in the Synchronization Editor:

1. In the Manager, select the **Universal Cloud Interface > Basic configuration data > Cloud applications** category.
2. Select the cloud application in the result list.

3. Select the **Change main data** task.
4. Select the **Edit synchronization project...** task.

Related topics

- Customizing the synchronization configuration on page 29

Container structures in cloud applications

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

To display a containers main data

1. In Manager, select the **Universal Cloud Interface > <cloud application> > Container structure** category.
2. Select the container in the result list.
3. Select the **Change main data** task.

You are provided with the following main data of a container. To handle manual provisioning operations, assign an application role for operators.

Table 16: Main 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	Text field for additional explanation.
Account manager	Manager responsible for the container.
Operators	Application role in which the cloud 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

Property	Description
	allowed to edit manual provisioning processes. Use the + button to add a new application role.

Related topics

- Cloud operators on page 88

User accounts in cloud applications

User accounts represent a cloud application's authentication objects. A user account obtains the necessary permissions for accessing cloud resources through its memberships in groups, system entitlements, and permissions controls.

Related topics

- Displaying user accounts on page 62
- Displaying assigned groups and system entitlements on page 66
- Displaying assigned permissions controls on page 66
- Displaying an overview of user accounts in cloud applications on page 67

Displaying user accounts

To display a user account's main data

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > User accounts** category.
2. Select the user account in the result list.
3. Select the **Show main data** task.

Detailed information about this topic

- General main data for user accounts in cloud applications on page 63
- Login credentials for user accounts in cloud applications on page 64
- Details of user account identification in cloud applications on page 64
- Contact data for user accounts in cloud applications on page 65
- User-defined main data for user accounts in cloud applications on page 65

General main data for user accounts in cloud applications

You are provided with the following general main data of a user account.

Table 17: General main data of a user account

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

Property	Description
Resource type	Type of the resource, for example, `user`.
Description	Text field for additional explanation.
Login name	Name the user uses for logging into the cloud application.
User account is disabled	Specifies whether the user account is locked.

Login credentials for user accounts in cloud applications

On the **Login** tab, enter the following main data.

Table 18: 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.

Details of user account identification in cloud applications

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

Table 19: Identification data for a user account

Property	Description
Street	Street or road.
Mailbox	Mailbox.
City	City.
Zip code	Zip code.
State	State.
Country	Country.

Property	Description
Address	Formatted postal address.
Language	Language and code identifier.
Time zone	Name of the time zone.
Room	Room.
Department	Identity's department
Division	Division the accounts belongs to.
Organization	Organization the accounts belongs to.
Personnel number	Number for identifying the identity, in addition to their ID.
Employment	Type of job.
Account manager	Manager responsible for the user account.

Contact data for user accounts in cloud applications

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

Table 20: Contact data for a user account

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

User-defined main data for user accounts in cloud applications

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

Table 21: Customized main data of a user account

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

Property	Description
	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.

Displaying assigned groups and system entitlements

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

To display assigned groups and system entitlements

1. In Manager, select the **Universal Cloud Interface > <cloud application> > User accounts** category.
2. Select the user account in the result list.
3. Select the **Assign groups and system entitlements** task.
4. Select the **Groups**, **System entitlements 1**, **System entitlements 2**, or **System entitlements 3** tab.

Related topics

- Groups in cloud applications on page 69

Displaying assigned permissions controls

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

To display assigned permissions controls

1. In Manager, select the **Universal Cloud Interface > <cloud application> > User accounts** category.

2. Select the user account in the result list.
3. Select the **Assign permissions controls** task.

Related topics

- Permissions controls in a cloud application on page 77

Displaying an overview of user accounts in cloud applications

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. In Manager, select the **Universal Cloud Interface > <cloud application> > User accounts** category.
2. Select the user account in the result list.
3. Select the **User account overview** task.

Groups and system entitlements in cloud applications

Groups and system entitlements represent the objects used in the cloud application to control access to the cloud resources. A user account obtains the necessary permissions to access cloud resources by assigning it to groups and system entitlements.

Detailed information about this topic

- System entitlements types in cloud applications on page 67
- Groups in cloud applications on page 69
- System entitlements in cloud applications on page 73

System entitlements types in cloud applications

Many cloud applications use different entitlement types to manage user entitlements. In addition to groups, these can also be roles or permissions sets, for example. Using synchronization projects created with the **Synchronization of a One Identity Starling Connect environment** project template, the different types are mapped in the One Identity Manager as follows.

Table 22: Mapping system entitlements in the One Identity Manager

Type	Table	Display name
Group	UCIGroup	Groups
Role	UCIGroup1	System entitlements 1
Profiles	UCIGroup2	System entitlements 2
Entitlement	UCIGroup3	System entitlements 3
Permissionset	UCIItem	Permissions controls

> NOTE: In synchronization projects created with a One Identity Manager version older than 8.2, objects of type **Profile** are also mapped in the `UCIItem` table.

A user account obtains the required entitlements for accessing target system resources through its assignments to groups or system entitlements. Depending on the target system, assignments are maintained either on user accounts (user-based assignment) or on system entitlements (entitlement-based assignment). When setting up synchronization using the **One Identity Starling Connect synchronization** project template, the SCIM connector determines the object type that stores the assignments. Memberships are mapped in the following tables:

Table 23: User-based assignment

`UCIUserHasGroup`	**Groups: Assignments to user accounts**
`UCIUserHasGroup1`	**System entitlement 1: Assignments to user accounts**
`UCIUserHasGroup2`	**System entitlement 2: Assignments to user accounts**
`UCIUserHasGroup3`	**System entitlement 3: Assignments to user accounts**
`UCIUserHasItem`	**User accounts: Permission control assignments**

Table 24: Entitlement-based assignment

`UCIUserInGroup`	**User accounts: Assignment to groups**
`UCIUserInGroup1`	**User accounts: Assignment to system entitlements 1**
`UCIUserInGroup2`	**User accounts: Assignment to system entitlements 2**
`UCIUserInGroup3`	**User accounts: Assignment to system entitlements**

Assignments for the `Permissionset` type are allows user-based.

By default, only groups are mapped by synchronization projects created with the **SCIM Synchronization** project template. The SCIM connector determines which object type stores the assignments and maps them accordingly either in the `UCIUserHasGroup` table or in the `UCIUserInGroup` table.

The types of system entitlements used and whether the assignments are saved with the user accounts or the system entitlements is stored with the cloud applications.

To display the types of system entitlements used

1. In the Manager, select the **Universal Cloud Interface > Basic configuration data > Cloud applications** category.
2. In the result list, select a cloud application and select the **Change main data** task.
   - **System entitlement types used**: List of types of system entitlements used in the cloud application.
   - **User account has memberships**: List of system entitlement types with user-based assignments. For types not listed here, the assignments are stored with the system entitlements.

> TIP: If the cloud application schema cannot be adequately represented by any default project template, customize the synchronization configuration. At the same time, define how the system entitlements are mapped in the One Identity Manager schema. When you are setting up synchronization, ensure that the base object for the cloud application (`CSMRoot`) is created in the database and the **System entitlements types used** (`GroupUsageMask`) and **User account has memberships** (`UserContainsGroupList`) properties are set correctly.

Related topics

- General main data for cloud applications on page 58

Groups in cloud applications

Groups and system entitlements represent the objects used in the cloud application to control access to the cloud resources. A user account obtains the necessary permissions to access cloud resources by assigning it to groups and system entitlements.

To display a group's main data

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > Groups** category.
2. Select the group in the result list.
3. Select the **Show main data** task.

To display a system entitlement's main data

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 1** category.

- OR -

In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 2** category.

- OR -

In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 3** category.

2. Select the system entitlement in the result list.
3. Select the **Show main data** task.

Detailed information about this topic

- General main data for groups in cloud applications on page 70
- User-defined main data for groups in cloud applications on page 71
- Displaying assigned user accounts on page 71
- Displaying assigned groups on page 72
- Displaying assigned permissions controls on page 72

Related topics

- System entitlements in cloud applications on page 73

General main data for groups in cloud applications

You are provided with the following general main data of a group.

Table 25: Entering main data of a group

Property	Description
Name	Name of the group.
Container	The group's container.
Cloud application	The group's cloud application.
Distinguished name	Distinguished name of the group.
Display name	Name for displaying the group in the user interface of One Identity Manager tools.
Group name	Additional name for the group.

Property	Description
Email address	Group's email address
Account manager	Manager responsible for the group.
Description	Text field for additional explanation.
Group type	Unique group type ID. For example if groups of different types are supplied through one and the same SCIM endpoint.
Resource type	Resource type identifier. The resource type corresponds to a SCIM endpoint, `/Groups` for example.

Related topics

- Groups in cloud applications on page 69

User-defined main data for groups in cloud applications

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

Table 26: User-defined main data of a group

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

Displaying assigned user accounts

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

To view assigned user accounts

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

Related topics

- User accounts in cloud applications on page 62
- Groups in cloud applications on page 69

Displaying assigned groups

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

To display assigned groups

1. In Manager, select the **Universal Cloud Interface > <cloud application> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign groups** task.
4. To display all groups that are members in the selected group, select the **Has members** tab.
5. To display all groups in which the selected group is a member, select the **Is member of** tab.

Related topics

- Groups in cloud applications on page 69

Displaying assigned permissions controls

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

To display assigned permissions controls

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > Groups** category.
2. Select the group in the result list.
3. Select the **Assign permissions controls** task.

Related topics

- Permissions controls in a cloud application on page 77
- Groups in cloud applications on page 69
-

Displaying an overview of groups in cloud applications

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

To obtain an overview of a group

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > Groups** category.
2. Select the group in the result list.
3. Select the **Group overview** task.

Related topics

- Groups in cloud applications on page 69

System entitlements in cloud applications

Groups and system entitlements represent the objects used in the cloud application to control access to the cloud resources. A user account obtains the necessary permissions to access cloud resources by assigning it to groups and system entitlements.

To display a system entitlement's main data

In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 1** category.

- OR -

In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 2** category.

- OR -

In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 3** category.

1. Select the system entitlement in the result list.
2. Select the **Show main data** task.

Detailed information about this topic

- General main data for system entitlements in cloud applications on page 74
- User-defined main data for user accounts in cloud applications on page 75
- Displaying assigned user accounts on page 75
- Displaying assigned system entitlements on page 76
- Displaying an overview of system entitlements in cloud applications on page 77

Related topics

- Groups in cloud applications on page 69

General main data for system entitlements in cloud applications

You are provided with the following main data for a system entitlement.

Table 27: General main data for a system entitlement

Property	Description
Name	Name of the system entitlement.
Container	Container for the system entitlement.
Cloud application	Cloud application of the system entitlement.
Distinguished name	Distinguished name of the system entitlement.
Display name	The display name is used to display the system entitlement in the One Identity Manager tools' user interface.
System entitlement name	Additional identifier for the system entitlement.
Email address	E-mail address of the system entitlement.
Account manager	Employee responsible for the system entitlement.
Description	Text field for additional explanation.
System entitlement type	Unique identifier of the system entitlement type, for example if system authorizations of different types are supplied through one and the same SCIM

Property	Description
	endpoint.
Resource type	Resource type identifier. The resource type corresponds to a SCIM endpoint, `/Roles` for example.

Related topics

- System entitlements in cloud applications on page 73

User-defined main data for user accounts in cloud applications

You can find customized data for a system entitlements on the **User defined** tab.

Table 28: User-defined main data of a system entitlement

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

Displaying assigned user accounts

Use this task to see all user accounts that are assigned to the system entitlement.

To display assigned user accounts

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 1** category.

   - OR -

In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 2** category.

- OR -

In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 3** category.

2. Select the system entitlement in the result list.
3. Select the **Assign user accounts** task.

Related topics

- User accounts in cloud applications on page 62
- System entitlements in cloud applications on page 73

Displaying assigned system entitlements

Use this task to see all system entitlements that are assigned to the system entitlement.

To display assigned system entitlements

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **System entitlements 1 overview** task, **System entitlements 2 overview** task, or **System entitlements 3 overview** task to match the selected system entitlement.
4. To display all system entitlements that are members in the selected system entitlement, select the **Has members** tab.
5. To display all system entitlements in which the selected system entitlement is a member, select the **Is member of** tab.

Related topics

- System entitlements in cloud applications on page 73

Displaying an overview of system entitlements in cloud applications

You use this task to obtain an overview of the most important information about a system entitlement.

To obtain an overview of a system entitlement

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 1** category.

   - OR -

   In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 2** category.

   - OR -

   In the Manager, select the **Universal Cloud Interface > <cloud application> > System entitlements 3** category.
2. Select the system entitlement in the result list.
3. Select the **System entitlement 1 overview** task, **System entitlement 2 overview** task, or **System entitlement 3 overview** task to match the selected system entitlement.

Related topics

- System entitlements in cloud applications on page 73

Permissions controls in a cloud application

Permissions controls map either system entitlements of the `Permissionset` type or any other cloud application objects.

To display a permissions control

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > Permissions controls** category.
2. Select the permissions control in the result list.
3. Select the **Show main data** task.

Detailed information about this topic

- General main data for permissions controls in cloud applications on page 78
- User-defined main data for permissions controls in cloud applications on page 78
- Displaying assigned user accounts on page 79
- Displaying assigned groups on page 79
- Displaying an overview of the permissions controls in cloud applications on page 80

Related topics

- System entitlements types in cloud applications on page 67
- Groups and system entitlements in cloud applications on page 67

General main data for permissions controls in cloud applications

Enter the following main data of a permissions control.

Table 29: General main data of permissions controls

Property	Description
Cloud application	Cloud application in which the permissions control applies.
Permissions control	Name of the permissions control.
Canonical name	Canonical name of the permissions control.
Distinguished name	Distinguished name of the permissions control.
Permissions type	Type of the permissions control.
Description	Text field for additional explanation.

Related topics

- Permissions controls in a cloud application on page 77

User-defined main data for permissions controls in cloud applications

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

Table 30: User-defined main data of permissions controls

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

Displaying assigned user accounts

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

To display assigned user accounts

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

Related topics

- User accounts in cloud applications on page 62
- Permissions controls in a cloud application on page 77

Displaying assigned groups

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

To display assigned groups

1. In the Manager, select the **Universal Cloud Interface > <cloud application> > Permissions controls** category.
2. Select the permissions control in the result list.
3. Select **Assign groups** category.

Related topics

- Groups in cloud applications on page 69
- Permissions controls in a cloud application on page 77

Displaying an overview of the permissions controls in cloud applications

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

To obtain an overview of a permissions control

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

6

Base data for managing cloud applications

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

- Target system types

  Settings for provisioning memberships and single objects synchronization are configured on the target system types. Target system types also map objects in the Unified Namespace.

  For more information, see Configuring the provisioning of memberships on page 35 and Configuring single object synchronization on page 36.

- Server

  Servers and their server functionality must be declared to handle cloud-specific processes in the One Identity Manager. For example, the synchronization server.

  For more information, see Job server for cloud-specific process handling on page 82.

- Cloud administrators

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

  For more information, see Cloud administrators on page 86.

- Cloud operators

  In One Identity Manager, you can assign identities to any cloud application to run provisioning manually. There is a default application role for cloud operators in One Identity Manager. Create more application roles if required.

  For more information, see Cloud operators on page 88.

- Cloud auditors

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

  For more information, see Cloud auditors on page 89.

Job server for cloud-specific process handling

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:

- In the Designer, create an entry for the Job server in the **Base Data > Installation > Job server** category. For more information about this, see the *One Identity Manager Configuration Guide*.
- In the Manager, select an entry for the Job server in the **Universal Cloud Interface > Basic configuration data > Server** category and edit the Job server main data category.

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

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

Related topics

- System requirements for the SCIM synchronization server on page 15

Editing Job servers for cloud applications

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.

To edit a Job server and its functions

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

Detailed information about this topic

- General main data for Job servers on page 83
- Specifying server functions on page 85

General main data for Job servers

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

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

Table 31: Job server properties

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

Property	Meaning
Parent Job server	Name of the parent Job server.
Executing server	Name of the executing server. The name of the server that exists physically and where the processes are handled. This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. The process steps are requested by the Job queue using this queue identifier. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values **Win32**, **Windows**, **Linux**, and **Unix** are permitted. If no value is specified, **Win32** is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the `QBM_PJobQueueLoad` procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more information, see the *One Identity Manager Process Monitoring and*

Property	Meaning
	Troubleshooting Guide.
Paused due to unavailability of a target system	Specifies whether task processing for this queue has been stopped because the target system that uses this Job server as a synchronization server is temporarily unavailable. As soon as the target system is available again, processing starts and all outstanding tasks are performed. For more information about offline mode, see the *One Identity Manager Target System Synchronization Reference Guide*.
No automatic software update	Specifies whether to exclude the server from automatic software updating. NOTE: Servers must be manually updated if this option is set.
Software update running	Specifies whether a software update is currently running.
Server function	Server functionality in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

Related topics

- Specifying server functions on page 85

Specifying server functions

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

The server function defines the functionality of a server in One Identity Manager. One Identity Manager processes are handled with respect to the server function.

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

Table 32: Permitted server functions

Server function	Remark
Update server	This server automatically updates the software on all the other servers. The server requires a direct connection to the database server that One Identity Manager database is installed on. It can run SQL tasks.

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

Related topics

- General main data for Job servers on page 83

Cloud administrators

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

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

Implementing the application role for cloud administrators

1. The One Identity Manager administrator appoints identities to be administrators for theUniversal Cloud Interface.

2. Cloud administrators add the identities to the default application role for operators and auditors.

   Administrators of the default application role are permitted to edit all cloud applications in One Identity Manager.

3. Administrators can authorize additional identities to be administrators and create child application roles as needed.

Table 33: Default application role for cloud administrators

User	Tasks
Cloud administrators	Cloud administrators must be assigned to the **Universal Cloud Interface | Administrators** application role or a child 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 cloud 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 identity as cloud administrator

1. Log in to One Identity Manager as a Manager administrator (**Base role | Administrators**)
2. Select the **One Identity Manager Administration > Universal Cloud Interface > Administrators** category.
3. Select the **Assign identities** task.
4. Assign the identity you want and save the changes.

To authorize additional identities as cloud administrators

1. Login to the Universal Cloud Interface with the **Manager | Administrators** application role.
2. In the **Universal Cloud Interface > Basic configuration data > Universal Cloud Interface managers > Administrators** category, select the application role.
3. Select the **Assign identities** task.
4. Assign the identity you want and save the changes.

Related topics

- One Identity Manager users for managing cloud applications on page 9
- Viewing and editing provisioning processes on page 54

Cloud operators

In One Identity Manager, you can assign identities to any cloud application to run provisioning manually. There is a default application role for cloud operators in One Identity Manager. Create more application roles if required.

Table 34: Default application role for cloud operators

User	Tasks
Cloud operators	The cloud operators must be assigned to the **Universal Cloud Interface | Operators** application role or a child 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 cloud operators' access permissions to individual cloud applications, define child application roles for each cloud application.

To specify cloud operators

1. Login to the Universal Cloud Interface with the **Manager | Administrators** application role.
2. Select the **Universal Cloud Interface > Basic configuration data > Cloud applications** category.
3. Select the cloud application in the result list.
4. Select the **Change main data** task.
5. On the **General** tab, select the application role in the **Operators** menu.

   - OR -

   Next to the **Operators** menu, click on + to create a new application role.

   - Enter the application role name and assign the **Universal Cloud Interface | Operators** parent application role.
   - Click **OK** to add the new application role.
6. Save the changes.
7. Assign identities, who are authorized to handle provisioning operations for this cloud application, to the application role.

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

To add identities to an application role

1. Login to the Universal Cloud Interface with the **Manager | Administrators** application role.
2. In the **Universal Cloud Interface > Basic configuration data > Universal Cloud Interface managers > Operators** category, select the application role.
3. Select the **Assign identities** task.
4. Assign the identities you want and save the changes.

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

Related topics

- General main data for cloud applications on page 58
- Container structures in cloud applications on page 61
- Editing pending provisioning processes on page 54
- One Identity Manager users for managing cloud applications on page 9

Cloud auditors

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

Table 35: Default application role for cloud auditors

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

To appoint identities to be cloud auditors

1. Login to the Universal Cloud Interface with the **Manager | Administrators** application role.
2. Select the **Universal Cloud Interface > Basic configuration data > Universal Cloud Interface managers > Auditors** category.
3. Select the **Assign identities** task.
4. Assign the identities you want and save the changes.

To create additional application roles for cloud auditors

1. Login to the Universal Cloud Interface with the **Manager | Administrators** application role.
2. Select the **Universal Cloud Interface > Basic configuration data > Universal Cloud Interface managers > Auditors** category.
3. Click 🗋 in the result list.
4. Edit the application role's main data.
    - Enter the application role name and assign the parent **Universal Cloud Interface | Auditors** application role or a child application role.
5. Save the changes.

Related topics

- Viewing all provisioning cases on page 55
- One Identity Manager users for managing cloud applications on page 9

Troubleshooting a cloud application connection

Error accessing the target system

Sometime accessing the target system returns the following error: `(429) Too Many Request`.

Probable reason

Some cloud applications block access to the target system for a certain period of time if there are too many requests. The above error is then displayed in the error log.

Solution

The SCIM connector tries to send the requests to the target system again after a certain period. Definitions according to RFC 6585 are observed. The connector retries up to 30 times.

Appendix A

Default project template for cloud applications

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

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

Detailed information about this topic

- Project template for SCIM on page 92
- Project template for One Identity Starling Connect on page 93

Project template for SCIM

Use the **SCIM synchronization** project template for synchronizing any System for Cross-domain Identity Management. The project template uses mappings for the following schema types.

Table 36: 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

Project template for One Identity Starling Connect

Use the **One Identity Starling Connect synchronization** project template for synchronizing SCIM using One Identity Starling Connect. The project template uses mappings for the following schema types.

Table 37: Mapping One Identity Starling Connect schema types to tables in the One Identity Manager schema

SCIM schema type	Table in the One Identity Manager Schema
Group	UCIGroup
User	UCIUser
Permissionset	UCIItem
Role	UCIGroup1
Profiles	UCIGroup2
Entitlement	UCIGroup3

Appendix B

Cloud system object processing methods

The following table describes permitted processing methods for SCIM schema types and the necessary restrictions for processing the system objects. By default, One Identity Manager allows all processing methods. Whether these processing methods can be used in the connected cloud application depends on the its implementation.

Table 38: Methods available for processing SCIM schema types

Schema type	Read	Paste	Delete	Refresh
User account (`User`)	Yes	Yes	Yes	Yes
Permissions control (`UCIItem`)	Yes	Yes	Yes	Yes
Group (`Group`)	Yes	Yes	Yes	Yes
System entitlement 1 (`UCIGroup1`)	Yes	Yes	Yes	Yes
System entitlement 2 (`UCIGroup2`)	Yes	Yes	Yes	Yes
System entitlement 3 (`UCIGroup3`)	Yes	Yes	Yes	Yes

Appendix C

Configuration parameters for managing cloud applications

The following configuration parameters are required.

Table 39: Additional configuration parameters

Configuration parameters	Meaning
QBM | PendingChange	General configuration parameter for configuring pending changes.
QBM | PendingChange | LifeTimeError	This configuration parameter specifies the maximum retention period (in days) for failed provisioning processes. The default is **30** days.
QBM | PendingChange | LifeTimeRunning	This configuration parameter specifies the maximum retention period (in days) for open provisioning processes. The default is **60** days.
QBM | PendingChange | LifeTimeSuccess	This configuration parameter specifies the maximum retention period (in days) for successful provisioning processes. The default is **2** days.
TargetSystem | CSM | ApplicationType	Configuration of the different cloud applications.
TargetSystem | CSM | ApplicationType | Salesforce	Salesforce application settings
TargetSystem | CSM | ApplicationType | Salesforce | DefaultProfileName	Name of the default profile assigned to new Salesforce users.

About us

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

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

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

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

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

Index