



One Identity Manager 8.1.3

Administration Guide for Connecting to Cloud Applications

Copyright 2020 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

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. 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.

Contents

Synchronizing cloud applications through Universal Cloud Interface	6
Architecture overview	7
One Identity Manager users for managing cloud applications	8
Setting up synchronization with a cloud application	10
Users and permissions for synchronizing with a cloud application	10
Setting up a synchronization server	11
Creating a synchronization project for initial synchronization of a cloud application	15
Displaying synchronization results	24
Customizing the synchronization configuration	24
How to configure cloud application synchronization	26
Updating schemas	26
Speeding up synchronization with revision filtering	27
Configuring the provisioning of memberships	28
Accelerating provisioning and single object synchronization	29
Help for the analysis of synchronization issues	30
Disabling synchronization	31
Base data for managing cloud applications	32
Administrators	32
Operators	34
Auditors	35
Editing a server	36
Master data for a Job server	37
Specifying server functions	40
Cloud applications	42
Cloud application master data	42
Alternative column names	44
How to edit a synchronization project	44
Container structures in a cloud application	45
User accounts in a cloud application	47
Additional master data for a user account	47

User account login data	49
Identification details	49
Contact data	50
User-defined master data	50
Additional tasks for managing user accounts	51
Overview of the user account	51
Assigning groups	51
Assigned permissions controls	52
Groups in a cloud application	53
Entering master data for a group	53
User-defined master data for a group	54
Additional tasks for managing groups	54
Overview of groups	55
Assigned user accounts	55
Assigning groups	55
Assigned permissions controls	55
Permissions controls in a cloud application	57
General master data for permissions controls	57
User-defined master data for permissions controls	58
Additional tasks for permissions controls	58
Permissions control overview	58
Assigned user accounts	59
Assigning groups	59
Provisioning object changes	60
The provisioning sequence	60
Displaying pending changes	61
Retention time for pending changes	62
Configuring manual provisioning	62
Managing provisioning processes in the Web Portal	64
Editing pending provisioning processes	65
Viewing and editing provisioning processes	66
Viewing all provisioning processes	66
Viewing statistics	66

Additional information for experts	68
Appendix: Default project template for cloud applications	70
About us	71
Contacting us	71
Technical support resources	71
Index	72

Synchronizing cloud applications through Universal Cloud Interface

One Identity Manager supports the implementation of Identity and Access Governance demands in IT environments, which are often a mix of traditional, internally hosted applications and modern cloud applications. Users and entitlements from cloud applications can be mapped in One Identity Manager.

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

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

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

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

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

The 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

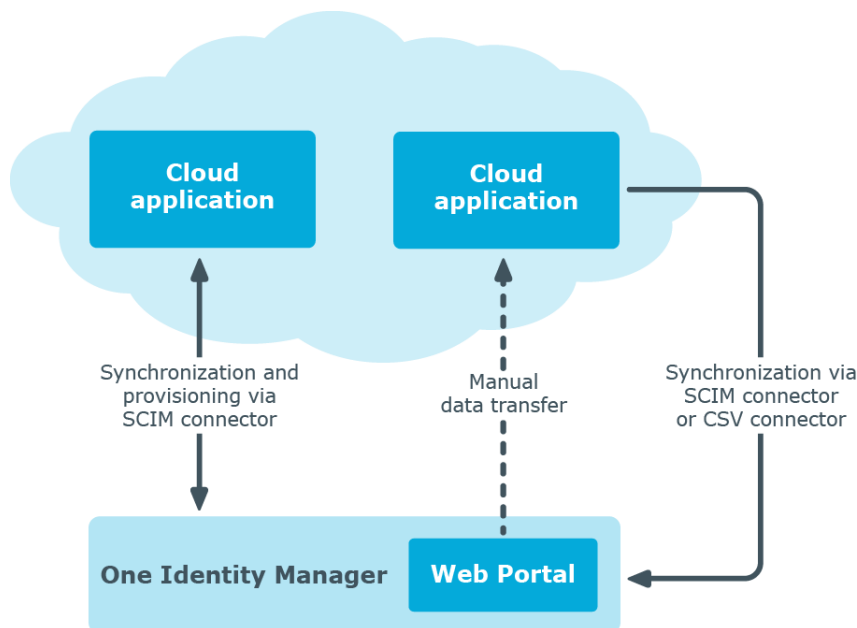
The synchronization of a cloud application with the One Identity Manager database and the provisioning of object changes from the One Identity Manager database to the cloud application is performed by the SCIM connector of One Identity Manager. This default method ensures that target system and database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

- Manual provisioning

For certain cloud applications, automated interfaces for provisioning changes can or should not be implemented. Changes can be manually provisioned for cloud application like this. For database transfer from the 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.

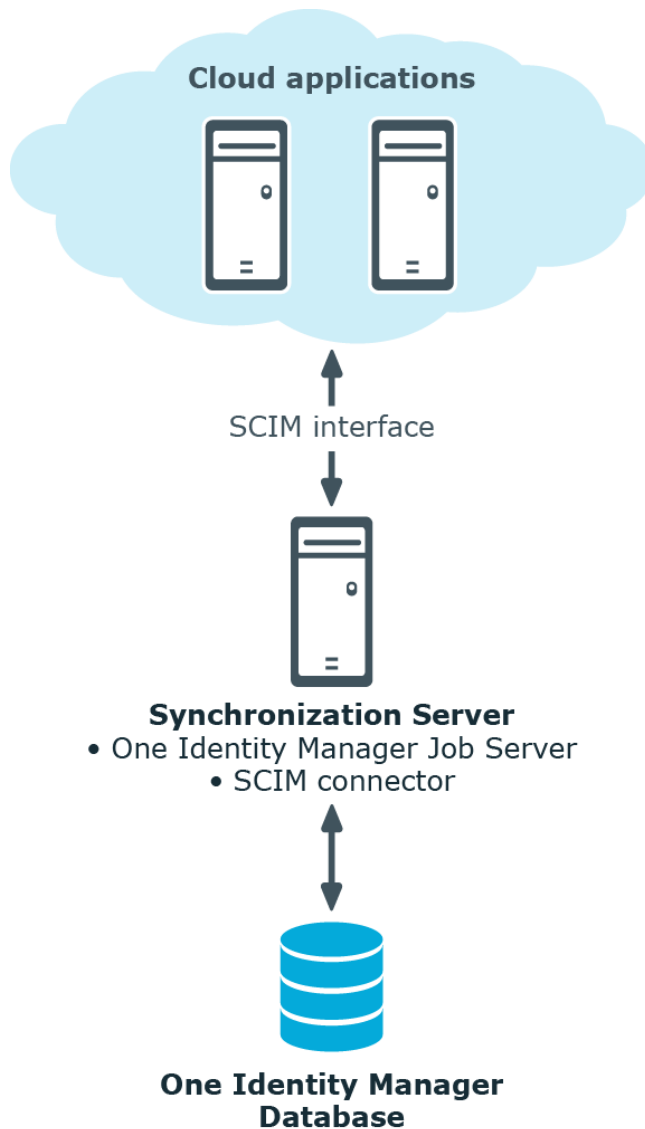
With the method, you carry the risk of inconsistent data and loss of data if manual processes are not carried out. This method is therefore not recommended.

Figure 1: Architecture for synchronization



To access cloud applications, the SCIM connector is installed on a synchronization server. The SCIM connector can communicate with cloud applications 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 synchronization with a cloud application](#) on page 10
- [Configuring manual provisioning](#) on page 62

One Identity Manager users for managing cloud applications

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

Table 1: Users

User	Tasks
Administrators	<p>Administrators must be assigned to the Universal Cloud Interface Administrators application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• 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.
Operators	<p>Operators must be assigned to the Universal Cloud Interface Operators application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Edit pending, manual provisioning processes in the Web Portal and obtain statistics.
Auditors	<p>Auditors must be assigned to the Universal Cloud Interface Auditors application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Can view manual provisioning processes in the Web Portal and obtain statistics.
One Identity Manager administrators	<ul style="list-style-type: none">• 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.• Create custom processes in the Designer as required.• Create and configure schedules as required.• Create and configure password policies as required.

Setting up synchronization with a cloud application

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

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

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

Detailed information about this topic

- [Users and permissions for synchronizing with a cloud application](#) on page 10
- [Setting up a synchronization server](#) on page 11
- [Creating a synchronization project for initial synchronization of a cloud application](#) on page 15

Users and permissions for synchronizing with a cloud application

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

Table 2: Users for synchronization

User	Permissions
One Identity Manager Service user account	<p>The user account for One Identity Manager Service requires permissions to carry out operations at file level. For example, assigning permissions and creating and editing directories and files.</p> <p>The user account must belong to the Domain users group.</p> <p>The user account must have the Login as a service extended user permissions.</p> <p>The user account requires access permissions to the internal web service.</p> <p>NOTE: If One Identity Manager Service runs under the network service (NT Authority\NetworkService), you can issue access permissions for the internal web service with the following command line call:</p> <pre>netsh http add urlacl url=http://<IP address>:<port number>/user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>The user account needs full access to the One Identity Manager Service installation directory in order to automatically update One Identity Manager.</p> <p>In the default installation, One Identity Manager is installed under:</p> <ul style="list-style-type: none">• %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	<p>Security tokens or user name and password for use as authentication in the cloud application.</p>
User for accessing the One Identity Manager database	<p>The Synchronization default system user is provided to execute synchronization with an application server.</p>

Setting up a synchronization server

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

- Windows operating system

The following versions are supported:

- Windows Server 2008 R2 (non-Itanium based 64-bit) service pack 1 or later
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
 - Windows Server 2019
 - Microsoft .NET Framework Version 4.7.2 or later
- | **NOTE:** Take the target system manufacturer's recommendations into account.
- Windows Installer
 - One Identity Manager Service, Synchronization Editor, SCIM connector
 - Install One Identity Manager components with the installation wizard.
 1. Select the **Select installation modules with existing database** option.
 2. Select the **Server | Job server | SCIM** machine role.

All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

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

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

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. 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 detailed information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

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

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

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

1. Start the Server Installer program on your administrative workstation.
2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager 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 One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using this unique queue identifier. 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 detailed information about configuring the service, see the *One Identity Manager Configuration Guide*.

- For a direct connection to the database:
 - a. Select **Process collection | sqlprovider**.
 - b. Click the **Connection parameter** entry, then click the **Edit** button.
 - c. Enter the connection data for the One Identity Manager database.
- For a connection to the application server:
 - a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
 - b. Click the **Connection parameter** entry, then click the **Edit** button.
 - c. Enter the connection data for the application server.

- d. Click the **Authentication data** entry and click the **Edit** button.
 - e. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
7. To configure remote installations, click **Next**.
 8. Confirm the security prompt with **Yes**.
 9. On the **Select installation source** page, select the directory with the install files.
 10. On the **Select private key file** page, select the file with the private key.
| NOTE: This page is only displayed when the database is encrypted.
 11. On the **Service access** page, enter the service's installation data.
 - **Computer:** Name or IP address of the server that the service is installed and started on.
 - **Service account:** User account data for the One Identity Manager Service.
 - To start the service under the **NT AUTHORITY\SYSTEM** account, set the **Local system account** option.
 - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation.
 - **Installation account:** Data for the administrative user account to install the service.
 - To use the current user's account, set the **Current user** option.
 - To use another user account, disable the **Current user** option and enter the user account, password and password confirmation.
 - To change the install directory, names, display names, or description of the One Identity Manager Service, use the other options.
 12. Click **Next** to start installing the service.
Installation of the service occurs automatically and may take some time.
 13. Click **Finish** on the last page of the Server Installer.
| NOTE: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

Creating a synchronization project for initial synchronization of a cloud application

Use the Synchronization Editor to set up synchronization between the One Identity Manager database and cloud application. The following describes the steps for initial configuration of a synchronization project.

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

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

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

Table 3: Information required for setting up a synchronization project

Data	Explanation
Server URL	URL for reaching the server including the transfer protocol.
Port	Port for accessing the cloud application.
URI service	URL for reaching the SCIM service.
Authentication endpoint or URL	URL available for authenticating. If authentication of another server or another root URL is used for authentication, the full URL must be entered here.
Authentication type	Permitted type of authentication for logging into the cloud application.
User account and password	User name and password for logging into the cloud application with the "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.
SCIM endpoint	Endpoint URIs or URLs for accessing the cloud application's schema, resource, and service provider data.
Synchronization server	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One

Data	Explanation
	<p>Identity Manager database are processed by the synchronization server.</p> <p>The One Identity Manager Service with the SCIM connector must be installed on the synchronization server.</p> <p>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.</p>

Table 4: Additional properties for the Job server

Property	Value
Server function	SCIM connector
Machine role	Server/Job server/SCIM

For more information, see [Setting up a synchronization server](#) on page 11.

One Identity Manager database connection data	<ul style="list-style-type: none"> • Database server • Database • SQL Server login and password • Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.
Remote connection server	<p>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.</p> <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none"> • One Identity Manager Service is started • RemoteConnectPlugin is installed • SCIM connector is installed

Data	Explanation
	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 <i>One Identity Manager Target System Synchronization Reference Guide</i> .

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

- Executed in default mode
- Started from the Launchpad

If you execute 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.

To set up initial synchronization project for a cloud application

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

NOTE: If synchronization is executed by an application server, connect the database through the application server.
2. Select the **Target system type SCIM interface** entry and click **Start**.
This starts the Synchronization Editor's project wizard.
3. On the **System access** page, specify how One Identity Manager can access the target system.
 - If access is possible from the workstation on which you started 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**.
4. On the **Configuration data** page, enter the connection parameters required by the SCIM connector to login to the cloud application.

Table 5: Server parameter

Property	Description
Server 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).

Property Description

Service URI	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. For example, if the full 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 user name and password.
OAuth Authentication	Authentication using the OAuth protocol 2.0.
Negotiated authentication (NTLM/Kerberos)	Authentication using Windows authentication methods such as NTLM or Kerberos.
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" in this case. If the base URL or the server is different to the resource URL, enter the full URL, for example "https://authserver.example.net/token".

- 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: Features of OAuth Authentication

Property	Description
Client secret	Security token for logging into the cloud application. If the client secret is not known, enter the user name and password.

Property	Description
User name and password	User name and password for logging into the cloud application if the security token is not known.
Application/client ID	The application/client ID used to register the cloud application with the security token service.
Grant type	Security token for logging into the cloud application with the "OAuth 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.
5. On **Verify 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.
6. On the **Endpoint configuration** page, enter the URIs for the SCIM end points. The SCIM default is used there is no URI.

Table 8: End point configuration

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

- 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.

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

Table 9: Local cache

Property	Description
Use local cache	<p>Specifies whether the SCIM connector's local cache is used.</p> <p>Local cache is used to speed up synchronization. Access to the cloud application is minimized during full synchronization. The option is ignored during provisioning.</p> <p>This option is set by default.</p> <p>It does not make sense to use the cache during synchronization with revision filtering. If the target system supports revision filtering, disable the option after initial synchronization.</p>

8. 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 V 2.0	Product for synchronizing a SCIM environment.
One Identity Starling Connect	Product for synchronizing a One Identity Starling Connect environment

9. 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.
10. 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.
11. 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.

12. 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.
13. 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 environment.
Synchronization of a One Identity Starling Connect environment	Use this project template for initial configuration of the synchronization project for synchronizing a SCIMenvironment using the 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.

14. 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
Read-only access to target system.	<p>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.</p> <p>The synchronization workflow has the following characteristics:</p> <ul style="list-style-type: none"> • Synchronization is in the direction of One Identity Manager. • Processing methods in the synchronization steps are only defined for synchronization in the direction of One Identity Manager.
Read/write access to target system. Provisioning available.	Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system.


Option	Meaning
--------	---------

The provisioning workflow displays the following characteristics:

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

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

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

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

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

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

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

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

The synchronization project is created, saved, and enabled immediately.

NOTE: If 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**.

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

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

To configure the content of the synchronization log

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

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

7. Click **OK**.

To synchronize on a regular basis

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

To start initial synchronization manually

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

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


Related topics

- [Setting up a synchronization server](#) on page 11
- [Users and permissions for synchronizing with a cloud application](#) on page 10
- [Displaying synchronization results](#) on page 24
- [Customizing the synchronization configuration](#) on page 24
- [Speeding up synchronization with revision filtering](#) on page 27
- [Additional information for experts](#) on page 68
- [Default project template for cloud applications](#) on page 70


Displaying synchronization results

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

To display a synchronization log

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Logs** category.
3. Click  in the navigation view toolbar.
Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking it.
An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Logs** category.
3. Click  in the navigation view toolbar.
Logs for all completed provisioning processes are displayed in the navigation view.
4. Select a log by double-clicking it.
An analysis of the provisioning is 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.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

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

Customizing the synchronization configuration

Having used the Synchronization Editor to set up a synchronization project for initial synchronization 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 master 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 methods, for example.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.

IMPORTANT: As long as 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.

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

Detailed information about this topic

- [How to configure cloud application synchronization](#) on page 26
- [Updating schemas](#) on page 26

How to configure cloud application synchronization

The synchronization project for initial synchronization provides a workflow for initial loading of Cloudtarget system objects (initial synchronization) and one for provisioning object modifications from the One Identity Manager database to the target system (provisioning). To use One Identity Manager as the master 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. Open the synchronization project in the Synchronization Editor.
2. Check whether existing mappings can be used for synchronizing the cloud application. Create new maps if required.
3. Create a new workflow with the workflow wizard.
This creates a workflow with **Target system** as its synchronization direction.
4. Create a new start up configuration. Use the new workflow to do this.
5. Save the changes.
6. Run a consistency check.

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. Open the synchronization project in the Synchronization Editor.
2. Select the **Configuration | Target system** category.
- OR -
Select the **Configuration | One Identity Manager connection** category.
3. Select the **General** view and click **Update schema**.
4. Confirm the security prompt with **Yes**.
This reloads the schema data.

To edit a mapping

1. Open the synchronization project in the Synchronization Editor.
2. Select the **Mappings** category.
3. Select a mapping in the navigation view.
Opens the Mapping Editor. For more detailed information about mappings, see the *One Identity Manager Target System Synchronization Reference Guide*.

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

Speeding up synchronization with revision filtering

When you start synchronization, all synchronization objects are loaded. Some of these objects have not been 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 its last execution date 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

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

To permit revision filtering for a start up configuration

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

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

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 in the target system as an object property in list form (Example: List of user accounts in the `members~value` property of a cloud group).
- 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. Select the **Configure tables for publishing** task.
3. Select the assignment tables that you want to set up for single provisioning. Multi-select is possible.
 - This option can only be enabled for assignment tables that have a base table with XDateSubItem or CCC_XDateSubItem column.
 - Assignment tables that are grouped together in a virtual schema property in the mapping must be marked identically.
4. Click **Merge mode**.
5. Save the changes.

For each assignment table labeled like this, the changes made in One Identity Manager are saved in a separate table. During modification provisioning, the members list in the target system is compared to the entries in this table. This means that only modified memberships are provisioned and 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 default 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.

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

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

Detailed information about this topic

- [Editing a server](#) on page 36

Help for the analysis of synchronization issues

You can generate a report for analyzing problems that arise during synchronization, inadequate performance for example. The report contains information such as:

- Consistency check results
- Revision filter settings
- Scope applied

- Analysis of the data store
- Object access times in the One Identity Manager database and in the target system

To generate a synchronization analysis report

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

The report may take a few minutes to generate. It is displayed in a separate window.

3. Print the report or save it in one of the available output formats.

Disabling synchronization

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

To prevent regular synchronization

1. Open the synchronization project in the Synchronization Editor.
2. Select the start up configuration and deactivate the configured schedule.

Now you can only start synchronization manually.

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

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

To deactivate the synchronization project

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

Detailed information about this topic

- [Creating a synchronization project for initial synchronization of a cloud application](#) on page 15

Base data for managing cloud applications

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

- Administrators

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

For more information, see [Administrators](#) on page 32.

- Operators

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

For more information, see [Operators](#) on page 34.

- Auditors

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

For more information, see [Auditors](#) on page 35.

- Server

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

For more information, see [Editing a server](#) on page 36.

Administrators

In One Identity Manager, you can assign employees to any cloud application, where they can synchronize it with One Identity Manager. There is a default application role for

administrators in One Identity Manager. Assign those employees to this application role who are authorized to configure synchronization and run manual provisioning. Create more application roles if required.


Table 13: Default application role for administrators

User	Tasks
Administrators	<p>Administrators must be assigned to the Universal Cloud Interface Administrators application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • 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 employee as administrator

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


To edit administrators

1. Select the **Universal Cloud Interface | Basic configuration data | Universal Cloud Interface Managers | Administrators** category.
2. Select the **Change master data** task.
 - OR -
 - Select an application role in the result list. Select the **Change master data** task.
 - OR -
 - Click  in the result list.
3. Edit the application role's master data.
 - Enter the application role name and assign the **Universal Cloud Interface | Administrators** parent application role or a child application role.

4. Save the changes.
5. Select the task **Assign employees** to assign members to the application role.
6. In the **Add assignments** pane, add employees.

TIP: In the **Remove assignments** pane, you can remove assigned employees.

To remove an assignment

- Select the employee and double-click .
7. Save the changes.

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

Related topics

- [Viewing and editing provisioning processes](#) on page 66

Operators

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


Table 14: Default application role for operators

User	Tasks
Operators	<p>Operators must be assigned to the Universal Cloud Interface Operators application role or a child application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none"> • Edit pending, manual provisioning processes in the Web Portal and obtain statistics.

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

To specify operators

1. Login to the 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 master 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 employees to this application role who are permitted to edit the cloud application in One Identity Manager.

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

To add employees to an application role

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

Related topics

- [Cloud application master data](#) on page 42
- [Container structures in a cloud application](#) on page 45
- [Editing pending provisioning processes](#) on page 65
- For detailed information about editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Auditors

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

Table 15: Default application role for auditors


User	Tasks
Auditors	Auditors must be assigned to the Universal Cloud Interface Auditors application role or a child application role.

User Tasks

Users with this application role:


- Can view manual provisioning processes in the Web Portal and obtain statistics.

To specify 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 **Change master data** task.
 - OR -
 - Select an application role in the result list. Select the **Change master data** task.
 - OR -
 - Click  in the result list.
4. Edit the application role's master 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.
6. Select the task **Assign employees** to assign members to the application role.
7. In the **Add assignments** pane, add employees.

TIP: In the **Remove assignments** pane, you can remove assigned employees.

To remove an assignment

- Select the employee and double-click .
8. Save the changes.

Related topics

- [Viewing all provisioning processes](#) on page 66

Editing a server

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

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

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

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

To edit a Job server and its functions

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

Detailed information about this topic

- [Master data for a Job server](#) on page 37
- [Specifying server functions](#) on page 40

Related topics

- [Setting up a synchronization server](#) on page 11

Master data for a Job server

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

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

Table 16: Job server properties

Property	Meaning
Server	Job server name.

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

Property Meaning

	This input is evaluated when the One Identity Manager Service is automatically updated. If the server is handling several queues, the process steps are not supplied until all the queues that are being processed on the same server have completed their automatic update.
Queue	Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
Server operating system	Operating system of the server. This input is required to resolve the path name for replicating software profiles. The values Win32 , Windows , Linux , and Unix are permitted. If no value is specified, Win32 is used.
Service account data	One Identity Manager Service user account information. In order to replicate between non-trusted systems (non-trusted domains, Linux server), the One Identity Manager Service user information has to be declared for the servers in the database. This means that the service account, the service account domain, and the service account password have to be entered for the server.
One Identity Manager Service installed	Specifies whether a One Identity Manager Service is installed on this server. This option is enabled by the QBM_PJobQueueLoad procedure the moment the queue is called for the first time. The option is not automatically removed. If necessary, you can reset this option manually for servers whose queue is no longer enabled.
Stop One Identity Manager Service	Specifies whether the One Identity Manager Service has stopped. If this option is set for the Job server, the One Identity Manager Service does not process any more tasks. You can make the service start and stop with the appropriate administrative permissions in the Job Queue Info program. For more detailed information, see the <i>One Identity Manager Process Monitoring and Troubleshooting Guide</i> .
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.
Last fetch time	Last time the process was collected.
Last timeout check	The time of the last check for loaded process steps with a dispatch value that exceeds the one in the Common Jobservice LoadedJobsTimeOut configuration parameter.

Property Meaning

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 40

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 17: 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. 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	This server can run SQL tasks. Several SQL processing servers can be set up to spread the load of SQL processes. The system distributes the generated SQL processes throughout all the Job servers with this server function.
CSV script server	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 on which reports are generated.

Server function	Remark
server	
SCIM connector	This server can connect to a cloud application.

Related topics

- [Master data for a Job server on page 37](#)

Cloud applications

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

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

To edit cloud application master data

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

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


Detailed information about this topic

- [Cloud application master data](#) on page 42
- [Alternative column names](#) on page 44

Cloud application master data

Enter the following master data for a cloud application.

Table 18: Cloud application master data

Property	Description
Cloud application	Name of the cloud application.
Canonical name	Full name of the cloud application. The canonical name is made up of the server's DNS name or its URL respectively, the port and the service's URI. Example: identities.example.net:8080/scim/v2
Distinguished name	The cloud application's distinguished name. This distinguished name is used to form distinguished names for child objects. Syntax example: DC = <canonical name>
Display name	Name for displaying the cloud application in One Identity Manager tools.
Operators	Application role in which the operators are defined. Operator edit manual provisioning processes for the cloud application that they are assigned to. Every cloud application can be assigned to other operators. Select the One Identity Manager application, whose members are allowed to edit manual provisioning processes. Use the  button to add a new application role.
Description	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 62
- [Managing provisioning processes in the Web Portal](#) on page 64

Alternative column names

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

To specify alternative column names

1. Select the **Universal Cloud Interface | Basic configuration data | Cloud applications** category.
2. In the result list, select a cloud application. Select the **Change master data** task.
3. Switch to the **Alternative column names** tab.
4. Open the membership tree in the table whose column name you want to change.
All the columns in this table are listed with their default column names.
5. Enter any name in the login language in use.
6. Save the changes.

How to edit a synchronization project

Synchronization projects in which a Cloud 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. Select the **Universal Cloud Interface | Basic configuration data | Cloud applications** category.
2. Select the cloud application in the result list. Select the **Change master data** task.
3. Select the **Edit synchronization project...** task.

Related topics

- [Customizing the synchronization configuration](#) on page 24

Container structures in a cloud application


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

To display a containers master data

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

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

Table 19: Master data for a container

Property	Description
Name	Container name.
Distinguished name	Container's distinguished name.
Parent container	Parent container for mapping a hierarchical container structure.
cloud application	The container's cloud application.
Description	Text field for additional explanation.
Account manager	Manager responsible for the container.
Operators	<p>Application role in which the operators are defined. Operators edit manual provisioning processes for the container that they are assigned to. Every container can be assigned to other operators.</p> <p>Select the One Identity Manager application, whose members are allowed to edit manual provisioning processes. Use the  button to add a new application role.</p>

Related topics

- [Operators](#) on page 34

User accounts in a cloud application

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

To display a user account's master data

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

Related topics

- [Additional master data for a user account](#) on page 47
- [User account login data](#) on page 49
- [Identification details](#) on page 49
- [Contact data](#) on page 50
- [User-defined master data](#) on page 50

Additional master data for a user account

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

Table 20: General master data for a user account

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

Property	Description
Form of address	User's form of address.
First name	The user's first name.
Last name	The user's last name.
Full name	Full name of the user account.
Initials	The user's initials.
Job description	The user's job description.
Nickname	Additional information about the user account.
Surname prefix	A prefix to the user's surname, for example "von" or "de".
Display name	User account display name.
Alias	Alias for further identification of the user account.
Name	User account identifier.
Container	User account's container.
First primary group	User account's primary group.
Second primary group	Additional primary group for the user account. If there are groups with different group types in the cloud application, another primary groups can be assigned.
Email address	User account's email address.
Email encoding	Type of email encoding.
Account expiry date	The date from which the user account can no longer be used to log in.
Resource type	Type of the resource, for example, user.
Description	Text field for additional explanation.
Login name	Name the user uses for logging into the cloud application.
User	Specifies whether the user account is locked.

Property	Description
----------	-------------

account is disabled	
---------------------	--

User account login data

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

Table 21: User account login data

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

Identification details

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

Table 22: Identification data for a user account

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

Property	Description
Department	Employee's department
Area	Area the accounts belongs to.
Organization	Organization the accounts belongs to.
Employee number	Number for identifying the employee, in addition to their ID.
Employment	Type of job.
Account manager	Manager responsible for the user account.

Contact data

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

Table 23: Contact data for a user account

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

User-defined master data

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

Table 24: Customized master data for a user account

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

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

Additional tasks for managing user accounts

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

Overview of the user account

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

To obtain an overview of a user account

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

Assigning groups

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

To display assigned groups

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

Related topics

- [Groups in a cloud application](#) on page 53

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. 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 57

Groups in a cloud application

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

To display a group's master data

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

Detailed information about this topic

- [Entering master data for a group](#) on page 53
- [User-defined master data for a group](#) on page 54

Entering master data for a group

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

Table 25: Entering master data for 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.

Property	Description
Display name	The display name is used to display the group in the One Identity Manager tools user interface.
Group name	Additional name for the group.
Email address	Group's email address
Account manager	Manager responsible for the group.
Description	Text field for additional explanation.
Group type	Name of the group type.
Resource type	Type of resource, for example, Group.

User-defined master data for a group

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

Table 26: User-defined master data for a group

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

Additional tasks for managing groups

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

Overview of groups

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

To obtain an overview of a group

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

Assigned user accounts

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

To view assigned user accounts

1. 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 a cloud application](#) on page 47

Assigning groups

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

To display assigned groups

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

Assigned permissions controls

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

To display assigned permissions controls

1. Select the **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 57

Permissions controls in a cloud application

Permissions controls map other cloud application objects.

To view a permissions control

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

Detailed information about this topic

- [General master data for permissions controls](#) on page 57
- [User-defined master data for permissions controls](#) on page 58

General master data for permissions controls

Enter the following master data for a permissions control.

Table 27: General master data for permissions controls

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

User-defined master data for permissions controls

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

Table 28: User-defined master data for permissions controls

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

Additional tasks for permissions controls

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

Permissions control overview

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

To obtain an overview of a permissions control

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

Assigned user accounts

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

To view assigned user accounts

1. Select the **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 a cloud application](#) on page 47

Assigning groups

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

To display assigned groups

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

Related topics

- [Groups in a cloud application](#) on page 53

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 can or should not be implemented. Changes can be manually provisioned for cloud application like this. The manual provisioning processes are displayed using a 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 execute, 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.

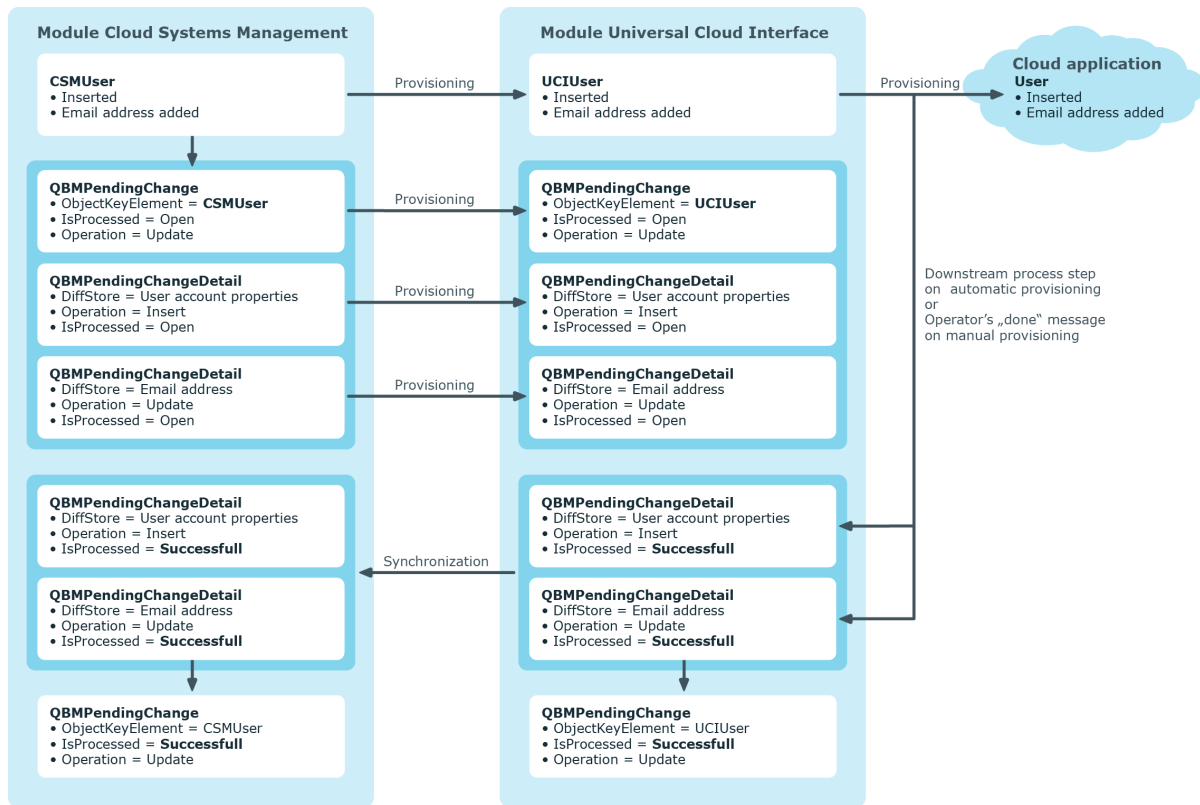
Detailed information about this topic

- [The provisioning sequence](#) on page 60
- [Configuring manual provisioning](#) on page 62
- [Retention time for pending changes](#) on page 62

The provisioning sequence

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

Figure 3: Provisioning sequence for pending changes



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

Displaying pending changes

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

To display pending changes

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

Table 29: Meaning of the icons in the toolbar

Icon	Meaning
	Show selected object.
	Reload the data.

Retention time for pending changes

Table 30: Configuration parameters

Configuration parameter	Effect when set
QBM PendingChange LifeTimeError	This configuration parameter specifies the maximum retention period (in days) for failed provisioning processes. Default is 30 days.
QBM PendingChange LifeTimeRunning	This configuration parameter specifies the maximum retention period (in days) for open provisioning processes. Default is 60 days.
QBM PendingChange LifeTimeSuccess	This configuration parameter specifies the maximum retention period (in days) for successful provisioning processes. Default is 2 days.

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

To configure the retention period for pending changes

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

Configuring manual provisioning

⚠ WARNING: Data may be lost through inconsistencies.

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

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

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

To configure manual provisioning

1. Edit the cloud application's master data.
 - a. Set the option **Manual provisioning**.
 - b. Assign the operators who are permitted to edit the open provisioning processes in the Web Portal.

TIP: You can also specify operators for individual containers. For more information, see [Container structures in a cloud application](#) on page 45.
2. Specify the auditors who are authorized to check manual provisioning processes in the Web Portal.

Detailed information about this topic

- [Cloud applications](#) on page 42
- [Cloud application master data](#) on page 42
- [Operators](#) on page 34
- [Auditors](#) on page 35
- [Editing pending provisioning processes](#) on page 65
- [Viewing all provisioning processes](#) on page 66
- [Setting up synchronization with a cloud application](#) on page 10

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

Managing provisioning processes in the Web Portal

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

Users can view or manage their entitlements, provisioning processes in the Web Portal, depending on which application roles they own. For more information, see [One Identity Manager users for managing cloud applications](#) on page 8.

To log into the Web Portal

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

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

Detailed information about this topic

- [Provisioning object changes](#) on page 60
- [Editing pending provisioning processes](#) on page 65
- [Viewing and editing provisioning processes](#) on page 66
- [Viewing all provisioning processes](#) on page 66

Editing pending provisioning processes

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

Table 31: Target objects

User account
Group
Assignment

NOTE: Administrators can also carry out pending provisioning processes.

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

Table 32: 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. Open the **Pending Cloud Operations** menu on the Web Portal's start page.
2. Mark the desired provisioning process in the **Pending Cloud Operations** view.
NOTE: If several operations are list under each other for the pending process marked in the operation detail, edit the first operation.
3. Carry out the instructions.
4. Click **Mark as Done**.

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

Viewing and editing provisioning processes

You can view all provisioning processes as administrator. This means, you can see pending and closed processes. You can edit pending processes but you cannot edit failed provisioning processes. For more information, see [Editing pending provisioning processes](#) on page 65.

To view provisioning processes

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

To view only provisioning processes.

1. Open **Pending Cloud operations**
2. Edit the process and click **Mark as done**.
Handled processes are moved to **Cloud Operations**.

Viewing all provisioning processes

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

To view provisioning processes

1. Open the **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 operation detail.

Viewing statistics

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

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

To view statistics

1. Double-click on a point in the timeline.
This opens a window with an enlarged visual 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 the **Help** link.
 - b. Select the **View source data** page.

Additional information for experts

When you set up synchronization with a cloud application, One Identity Manager uses the SCIM schema exported from the server. If the SCIM connector cannot find the schema, you can pass it the schema data by using override files. The override files contain a complete description of the schema being used and they must conform 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 15. 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 (manual)** page, enter the path for the override files. Both files must exist.

Table 33: Information about override files

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

- 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. Open the synchronization project in the Synchronization Editor.
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. Open the synchronization project in the Synchronization Editor.
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.

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.

The template uses mappings for the following schema types.

Table 34: 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

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

A

- account manager 49
- administrator 8, 32
- application role 8
 - administrator 32
 - auditor 35
 - operator 34
- auditor 8, 35, 62

C

- calculation schedule
 - disable 31
- cloud application 42
 - alternative column description 44
 - delete user account 42
 - manual provisioning 42
 - operator 42
 - user 8
- container 45
 - account manager 45
 - operator 45

D

- direction of synchronization
 - direction target system 15, 26
 - in One Identity Manager 15

G

- group 53
 - account manager 53

- assigned groups 55
- assigned permissions controls 55
- assigned user accounts 55
- container 53
- group type 53

J

- Job server
 - load balancing 29
 - properties 37

L

- load balancing 29
- local cache 15

M

- membership
 - modify provisioning 28

O

- operator 8, 34, 62
- override file 68

P

- pending changes 60-61
 - retention period 62
- permissions control 57
 - assigned groups 59
 - assigned user accounts 59

- permissions type 57
- project template 70
- provisioning 60
 - accelerate 29
 - manual 62
 - members list 28
- provisioning process 62
 - delete 62
 - display 61
 - failed 61
 - open 61

R

- resource configurations 68
- revision filter 27

S

- schema
 - changes 26
 - shrink 26
 - update 26
- schema definition 68
- server function 40
- single object synchronization
 - accelerate 29
- synchronization
 - accelerate 27
 - authorizations 10
 - configure 15, 24
 - connection parameter 15, 24
 - only changes 27
 - prevent 31
 - scope 24
 - set up 10

- start 15
- synchronization project
 - create 15
 - user 10
 - user cache 15
 - workflow 15, 26
- synchronization analysis report 30
- synchronization configuration
 - customize 24, 26
- synchronization log 24
- synchronization project
 - create 15
 - disable 31
 - edit 44
 - project template 70
- synchronization server 36
 - configure 11
 - install 11
 - server function 40
- synchronization workflow
 - create 15, 26

U

- user account 47
 - account manager 49
 - assigned groups 51
 - assigned permissions controls 52